LEGION
Cyberworks
Protect | Adapt | Survive

Security Program Assessment

Process Overview

Introduction

Our clients are often sophisticated and goal oriented in terms of how they approach information security. Many have implemented a top-down approach to managing risk and their C-Suite and Boards are providing Governance. They are involved in the formation and/or approval of the organization’s overall mission, goals, and strategy pertaining to information security. The result of this Governance (the Policies, Guidelines, Procedures, People, Controls, and the associated Budgets) collectively, is your Security Program.

Our Security Program Assessment (SPA) service is a valuable addition to, or a replacement for, your internal processes of reviewing, validating, and improving your Security Program, giving your organization an objective, experienced third-party evaluation, which is often a requirement for annual certification and compliance.

The SPA engagement deliverable is a report of findings and associated recommendations for how your organization can achieve compliance and improve your overall security program across the five fundamental areas of Cybersecurity: Identify, Protect, Detect, Respond, and Recover.

Discovery

We start with discovery where we collect the essential information needed for the remainder of the engagement. Follow up sessions are conducted, as needed, to get clarification on any questions and outstanding items. The main objectives of the discovery phase are as follows:

- Gain an understanding of your business and how you use technology, and get to know you and your unique organizational profile
- Capture your business goals and priorities pertaining to information security and privacy, and compliance with applicable state and federal laws
- Develop a high-level description of your Information Security Program (Policies, Guidelines, Procedures, People, and Controls)
- Learn about your biggest cybersecurity pain points, known issues, and the cybersecurity challenges facing your organization.

Assess & Audit

We review your Policies, Guidelines, Procedures, Staffing, and your Controls to evaluate them against state and federal laws and your stated business goals and priorities pertaining to information security and privacy.

During this interactive table-top Q & A exercise, we review your administrative, technical, and physical security controls, covering 20+ categories and more than 95 individual sub-controls. This is a comprehensive discussion conducted at your place of business that will require participation from SMEs in the areas of servers, networking, remote access, operating systems, automation, cloud, applications, the flow of information and data across your systems and networks, and other areas, depending on your specific organizational and technology environment makeup.

Findings & Recommendations

The information collected during the Assess & Audit exercise is reviewed and compared against best practices as well as against security and privacy requirements in applicable state and federal laws such as HIPAA, HI-TECH, PCI, and SEC’s Regulation S-P.

From this review, we develop a list of findings where there are deviations with following best practices, meeting your stated security and privacy goals, or in areas of non-compliance with state or federal privacy and security laws.

Finally, we provide recommended actions that you can take to close out any findings and to align your Security Program with best practices and recognized frameworks, such as those from NIST and the Center for Internet Security.

As a full-service security and infrastructure services and solutions provider, we can assist you with acquiring and/or implementing technologies, methods, tools, and the know-how to close out findings and achieve your information security goals and mission.

Legion Cyberworks LLC

919-769-2916

info@legioncyber.com