Cyber Security Program

PLETHORA offers to design a compliant **cyber security program** customized to your business requirements**.** We help you in creating and implementing the Cyber Security program.

Problem

- Shortage of technical and operational experience in Cyber Security is a huge roadblock for decision-making. Businesses has to answer the tough questions: **What are the security problems, the Cyber Risks, and What is the worst-case scenario?**
- We will help you explore answers **by assessing security risks, understanding the threats, prioritizing practical efforts, and defining risk treatment and acceptance approaches.**

Service Overview

- **Assess Your Security Program**
  Assess your existing security program against best practice framework "NIST Cyber Security Framework". Recommendations are made based on any gaps or improvements to be made in the security program based on the Cyber Security frameworks and are used to develop a roadmap to achieving your ideal security program state.
- **Understand Your Current State, build a Plan for Progress**
  A thorough security program assessment is the first step toward developing a more efficient security program. Use a security program assessment as a tool to create a timeline and roadmap to bringing your security program to an ideal state with mind to regulatory and customer requirements as well as organizational initiatives.
- **Develop Your Security Program**
  Once you have received your custom roadmap, build or improve your security program with your in-house team. If you don't have your in-house security resources or expertise then our expert security team will put together the different parts of your security program components.

Key Benefits

- Experienced Infosec Team will develop Security program for your business.
- We understand both your Business and Security needs to prioritize the activities.
- We will help you to measure the ROI of Cyber security investments.

How it works

- **Discovery Phase**
  The first step in creating a security program is understanding what you have, what you need and what you need to protect. Risk assessments, gap analyses, security testing are all helpful in this initial planning phase to understand your next steps, accurate resource allocation and budgets going forward.
- **Program Development Phase**
  With a full plan in place, our security team can begin recommending your security controls, Cyber Security technology or tools and writing your policies and procedures.
- **Normal Business Operations**
  Once your security program is in place and fully functioning, your data, systems and users will be protected by a robust system for mitigating risks, alerting your team to threats and preventing breaches that put your business at risk.

REQUEST A CONSULTATION

Scope Definition

Name of the Organization/Company:	
Business Industry:	
Approx. Number of Total Employees:	
Approx. Number of the Subsidiaries or the Sister concerns of the Organization/Company:	
Approx. Number of the Vendors/Partners/Suppliers:	
List the Business Domain(s):	
List the Email Domain(s):	
Location of Office Headquarters:	
Locations of Business Operations:	
Locations of Subsidiaries or the Sister concerns:	
Services Required: • Gap Assessment & Reporting (Y/N) • Implement Cyber Security Framework Consulting (Y/N) • Tool/Platform (Y/N) • Policies Development (Y/N) • Dedicated Cyber Security Consultant (Y/N)	