FAQ

• Why do I need a cybersecurity program?
Every product found on the shelf of every store today was conceived, designed, manufactured, marketed, and distributed by the use of technology. Known as Digital Transformation, this quiet revolution has left every company vulnerable to digital attacks that can literally end their business.

• What are the benefits of having a cybersecurity program?
A cybersecurity program is an organized approach to managing cyber risks. Unlike cybersecurity in general, a program revolves around your people, products and processes. it's not a technology solution, it's a repeatable and sustainable system designed to uncover vulnerabilities and address them in order to reduce risk in a more holistic manner. Recent evidence has shown companies that employ best practice frameworks and have cybersecurity programs in place are winning more bids.

• What are the benefits of working with us?
Standing up a NIST based cybersecurity program can take years for an inexperienced team, and the cost of hiring a full-time cybersecurity professional can be high, if you can find one. After initiating and running several successful programs we have learned how to streamline the process in order to focus on the outcome. Because of this we are able to take you from doing nothing, to doing the right things in a very short period of time.

• What is the resource commitment required?
Flexible Program Development is designed to get your program off-the-ground. This step usually takes 40 hours with two of our staff and two of yours, and starts around $20,000 depending on the size and complexity of your organization.

• Are there additional services offered?
We offer, and encourage clients to get employee awareness training, privileged user training, and a full risk assessment.

About Us

GRALOC, LLC. is a family business that was formed in 2019 around a distinct vision to bring sophisticated cyber risk management to the small business community. After decades spent managing cybersecurity for Critical Infrastructure such as manufacturing, energy, and water the founders realized that resilience and survival were critical to every business. The continued existence of the small business is under an increasing threat from larger competitors with the resources to direct at managing risk. However, it is not a matter of resources, the small business has been the backbone of our economy because of its ability to evolve, and with the proper knowledge and focus we can help these organizations meet this challenge as well. Our mission is to level the playing field for the small business and give them the tools to thrive in this new environment.

GRĀLOC

contact
PHONE (719) 271-3624

online
SHAWN@GRALOC.COM
WWW.GRALOC.COM

GRĀLOC

REDUCE RISK. ADD VALUE. GAIN ADVANTAGE.

FLEXIBLE PROGRAM DEVELOPMENT

Puts you in charge of your NIST-CSF program development.

What is NIST-CSF

The NIST Cybersecurity Framework (CSF) was originally developed for the enhanced cyber protection of the nation's critical infrastructure. It was designed to be a cost-effective method for securing systems and facilities against cyber threats that could disrupt services that are critical to people. Since its introduction in 2014 it has grown to become a standard framework for business and government. Cybersecurity programs based on the NIST-CSF have the advantage of using a common reporting method and can be articulated to customers and partners in a language that is familiar to them.

The inevitable spread of the NIST-CSF from government and critical infrastructure to their suppliers has accelerated its inclusion in new vendor requirements designed to strengthen the supply chain. NIST has recently found its way into the boardrooms of the fortune 1000 and is beginning to shape instruments such as insurance policies, and financial disclosures. In the past few years, adoption of the NIST-CSF has enabled many businesses to compete on government contracts with very favorable results. NIST, a framework originally designed to improve a weakness in our infrastructure now seems poised to underpin many aspects of the digital economy.

Our Process

Let's start by dispelling a few myths. Cybersecurity is not an IT function, nor is it just about hackers and technology. It's about your people and your culture, and ultimately, it's about your ability to adapt and overcome adversities that threaten your mission and vision. Building an effective cybersecurity program is a process of gaining insights into your business, how it operates, its weaknesses, and its strengths.

Before we begin the process, your company will have to choose a champion who can lead the effort as the program manager. You will also need a small team of two or more employees from diverse areas of the company who will help steer the program. These positions are part-time, and the team usually meets once a month.

The new cyber-team will be trained on risk management and program mechanics. We will then install a few company policies, guidelines, and SOP's. We will conduct the initial guided self-assessment which will give you a current NIST profile and tier. Based on the assessment results we will prioritize areas of concern and develop the Cybersecurity Plan with specific initiatives designed to address those concerns. This cybersecurity plan will enable the creation of your target NIST profile and tier.

This may seem a bit daunting, but we have developed a structured process that is designed to move the needle quickly and incrementally. Working with us is a partnership, together we discover and mitigate vulnerabilities and along the way you will learn how to operate an effective cybersecurity program.

The Details

FLEXIBLE PROGRAM DEVELOPMENT

CYBER PROGRAM TRAINING

Cyber Risk Management Strategy
Cybersecurity Program Fundamentals
NIST Framework Basics

GUIDED SELF ASSESSMENT

Conduct assessment based on NIST framework core. Score the assessment and establish your current NIST profile and tier

POLICY INSTALLATION

Install cybersecurity policy, program policy and charter, accepable use policy, password guidelines, and a few standard operating procedures

PLANNING & REPORTING

Prioritize areas of highest risk, create your target NIST profile and document initiatives in a Cybersecurity Plan