![Systems Engineering Employee-Owned logo]

SYSTEMS
engineering
Employee-Owned

THE SYSTEMS ENGINEERING

Adaptive Cybersecurity Framework (aCSF)

Building a Strong Foundation for
Growing Cybersecurity Maturity

NIST CSF assessed and operationalized
to embed security across organizations

TODAY'S IMPERATIVE: GROW YOUR SECURITY STRENGTH

In today's digital world, a single cybersecurity incident can devastate the productivity, profitability, and reputation of your organization. Yet, many organizations struggle to develop a strong cybersecurity posture due to constantly evolving cybersecurity threats, limited budgets, and a short supply of skilled cybersecurity workers. To keep pace with today's threats, as well as burgeoning client, regulatory, and cybersecurity insurance requirements, an increasing number of organizations are choosing managed technology services to act as their IT and security department or supplement their internal technical skillsets.

SECURITY IS A JOURNEY: ENSURE STRONG ROOTS

Solving the People, Process, Tech Equation

Technology services are just the beginning of robust security–your organization, and your managed technology services provider , must also continuously improve people, processes and technology to maintain a strong cybersecurity posture. Since no organization is ready to do everything at once, you need a continuous improvement approach that may take months or even years depending on where you are starting from and how aggressive you need to be – we can help.

SE aCSF Overview: Standards Based Security

With this in mind, we developed SE aCSF, an innovative approach that provides your organization with the technology and support you need today, combined with an ongoing review to identify and prioritize actions and measurement of your progress based on the widely adopted NIST Cybersecurity Framework (NIST CSF). The result is an increase in cybersecurity maturity and bolstered resilience throughout your organization.

SYSTEMS ENGINEERING ADAPTIVE CYBERSECURITY FRAMEWORK
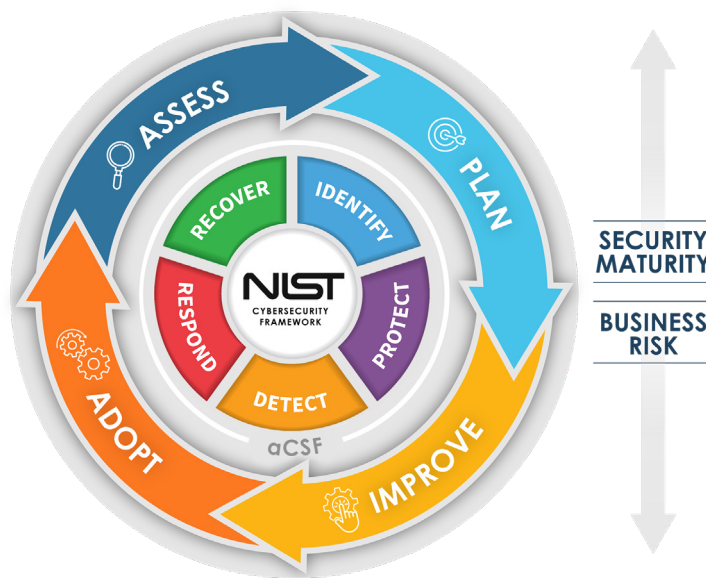
THE IMPORTANCE OF THE NIST CSF

The NIST CSF is the leading framework to help organizations manage cybersecurity risks using a flexible framework of standards, guidelines, and practices. It helps organize policies and build a strong cybersecurity posture in its five key activity areas: Identify, Protect, Detect, Respond, and Recover.

NIST is the underlying standard for information security for most regulatory requirements including HIPAA, FISMA, GLBA and more.

NIST: FULLY OPERATIONALIZED

While the flexibility of the NIST CSF enables any organization to use it as a strategic planning and assessment tool, the guidance is often ambiguous, and it can be difficult to understand how to apply the framework to your organization's unique environment. With these challenges in mind, we developed aCSF to:

1 Operationalize the NIST CSF into our managed technology services to deliver long-range cybermaturity enhancements to our IT services and your organization, regardless of your adoption, or not, of the framework.

2 Provide the professional guidance to go beyond the fundamentals and adopt NIST CSF as your information security framework.

SE aCSF ensures a security first and integrated approach for all our clients.

REVOLUTIONIZING MANAGED TECHNOLOGY SERVICES

SE aCSF was developed to revolutionize managed technology services. Our experienced team has found that one of the biggest predictors of a successful long-term security program is to make it part of your culture and to continuously increase the cybersecurity maturity of your people, process, and technology. To make this possible, our security experts spent nine months developing and operationalizing a proprietary 200+ point methodology based on the NIST CSF and infused it into our managed services.

THE UNSURPASSED SERVICE YOU DESERVE: DELIVERED SECURELY

While all our clients receive the benefits of superior security from our continuous NIST CSF internal improvements, coupled with our network assessment, excellent project management, and super service delivery, with SE aCSF you also get:

Initial Maturity Measurement

Our team explains where you are on the cybermaturity scale and notes areas and a roadmap for improvements.

Maturity Planning

You will receive recommendations for next steps in your security maturity planning and can elect to add some additional, optional continuous cybersecurity maturity improvement services.

Benchmarking

We'll provide benchmarking to guide your improvements.

Bi-Annual Review

Get expert guidance on industry trends, threat landscape changes, and advice on how these changes can impact your organization.

THE BENEFITS OF SE aCSF

An increasing number of clients, partners, and cyber insurers contractually require vendors and partners to maintain minimum cybersecurity standards. Public companies are facing even more scrutiny with new regulatory rules regarding cybersecurity risk management and reporting. SE aCSF helps your organization stay secure and meet these obligations by delivering a NIST CSF-aligned security program that:

Protects productivity
by reducing your organization's risk of a disruptive and potentially financially damaging cybersecurity incident.

Simplifies compliance reviews
a structured cybersecurity program that facilitates smoother audits.

Delivers prioritized guidance
with initial maturity measurement, benchmarking, and reviews.

An in-depth Cyber Risk Assessment
when you are ready to fully adopt NIST CSF.

GETTING STARTED

When you engage our aCSF managed technology services, you will be assigned a team of experts who will seamlessly integrate our services with your unique environment.

SE aCSF delivers the ultimate shared security managed services. We deliver strong, NIST CSF-aligned and continuously evolving managed technology services that protect your business, as well as the professional guidance you need to continuously improve your cybersecurity and resilience.

CONTACT US

Contact us for more information about how we can help protect your organization from current, emerging, and future cybersecurity threats.

888.624.6737
info@systemsengineering.com
systemsengineering.com

ABOUT SYSTEMS ENGINEERING

Systems Engineering is an employee owned, SOC2, Type 2 certified IT strategy and managed services provider dedicated to enabling the exceptional in clients with offices in Portland, Maine, and Manchester, New Hampshire. From network design and installation to a full complement of managed IT, cybersecurity, and cloud services, we have IT solutions that enable organizations to reach their full potential.

System Engineering's team of 180+ US network engineers, managed security professionals, project managers, data management experts, and account managers are available 24×7, 365 days per year to meet the needs of our clients.