360 CYBER PROGRAM
OVERVIEW

INFO@360ADVANCED.COM 360ADVANCED.COM (866) 418-1708

TABLE OF CONTENTS

WHO WE ARE

We are a solution-centric professional services firm that helps enterprise organizations develop, implement and maintain cybersecurity and compliance programs that are aligned with strategic objectives, tailored to each industry's regulatory requirements, and carefully designed to maximize return on investment.

Founded in 2004 and headquartered in St. Petersburg, Florida, 360 Advanced, Inc. is a licensed Certified Public Accounting (CPA) firm, an approved HITRUST CSF® Assessor (and a member of the HITRUST Authorized External Assessor Council and Quality Subcommittee), a member of the Cloud Security Alliance, and an authorized Payment Card Industry Qualified Security Assessor (PCI QSA), specializing in information technology assurance and compliance.

Few other firms have this combination of credentials. Accordingly, we offer a unique blend of integrated services commonly desired but rarely delivered by a single provider.

Led by former "Big 4" executives, 360 Advanced has a **staff of 80+,** and is organized with reporting structures of Directors, Managers, Seniors, and Staff Associates. **With diverse technical backgrounds, our team has the distinctive ability to undertake complex, enterprise level projects that span multiple business units, geographic locations, and environments.**

FIRM ACCREDITATIONS & LICENSES

TEAM CREDENTIALS

Teams are assembled based on a targeted mix of skills and experience to meet the needs of your project.

Our professionals have a unique blend of accounting, technology, audit, security, and management consulting experience specific to one or more of our disciplines. And, with years of experience and a variety of professional certifications, we are well equipped to help you meet your cybersecurity and compliance needs.

- A+
- AWS CCP
- CASP+
- CBCP
- CCENT
- CHQP
- CCSFP
- CDPO
- CDPSE
- CEH
- CTT+
- CISM
- CISSP
- COBIT 5
- COMPTIA SEC
- CPA
- CRISC
- CSIS
- CISA
- CISSP
- EWPT
- HCISP
- ITIL
- MACC
- OSCP
- OSWP
- PCIP
- PWAPT
- QSA
- CERTIFIED SCRUM MASTER
- CISCO PACKET TRACER
- ISO 22301 LEAD AUDITOR
- ISO 27001 LEAD AUDITOR
- ISO 27001 LEAD IMPLEMENTER
- SECURITY + CE

360 CYBER PROGRAM

Program Overview

360 CYBER helps your organization understand dynamic Cybersecurity & Compliance challenges, adapt and respond to the risks inherent in your business ecosystem, and protect the assets most critical to your brand, competitive advantage, and shareholder value. We provide subject matter and industry guidance related to cybersecurity, regulatory/ industry framework compliance, and enterprise customer expectations. Through collaboration with management, we develop a customized cybersecurity controls framework that fits your specific environment, compliance requirements, and customer expectations.

WHY 360 CYBER

Common Challenges

A LACK of resources and/or expertise to utilize the full potential of your cybersecurity and compliance technology platform

AN UNCLEAR understanding of your organization's security & compliance obligations

HOW TO implement sufficient controls to meet security & compliance requirements

A DISCONNECT between current IT and cyber programs and compliance

---

The 360 CYBER Solution

A DEDICATED partner and personnel to streamline your compliance risk assessment process to ensure current and future compliance obligations are being met

INTEGRATE COMPLIANCE with current IT and cyber programs to improve organizational efficiency, which saves time and money

BRING COMPLIANCE objectives into the discussion with your executives and board

REDUCE the legal and reputational risk to your organization

TURN compliance into a competitive advantage instead of an organizational burden

COORDINATE with your audit partners to facilitate and simplify the audit process

WHAT WE OFFER

360 CYBER Services

Security Program

Evaluation & Roadmap

Privacy & Risk Management

Compliance Support

Architect a Secure IT environment

Information Security Leadership & Guidance

Steering Committee Leadership or Participation

Executive Leadership Presentations

Security Compliance Management

Incident Response Support

Third-Party Vendor Management

Monthly | Quarterly | Annual Reviews

Deliverables

Compliance Readiness

Security Policy & Procedure Development

Internal Audit

Security Awareness Training

Incident Response Plan

Security Risk Assessment

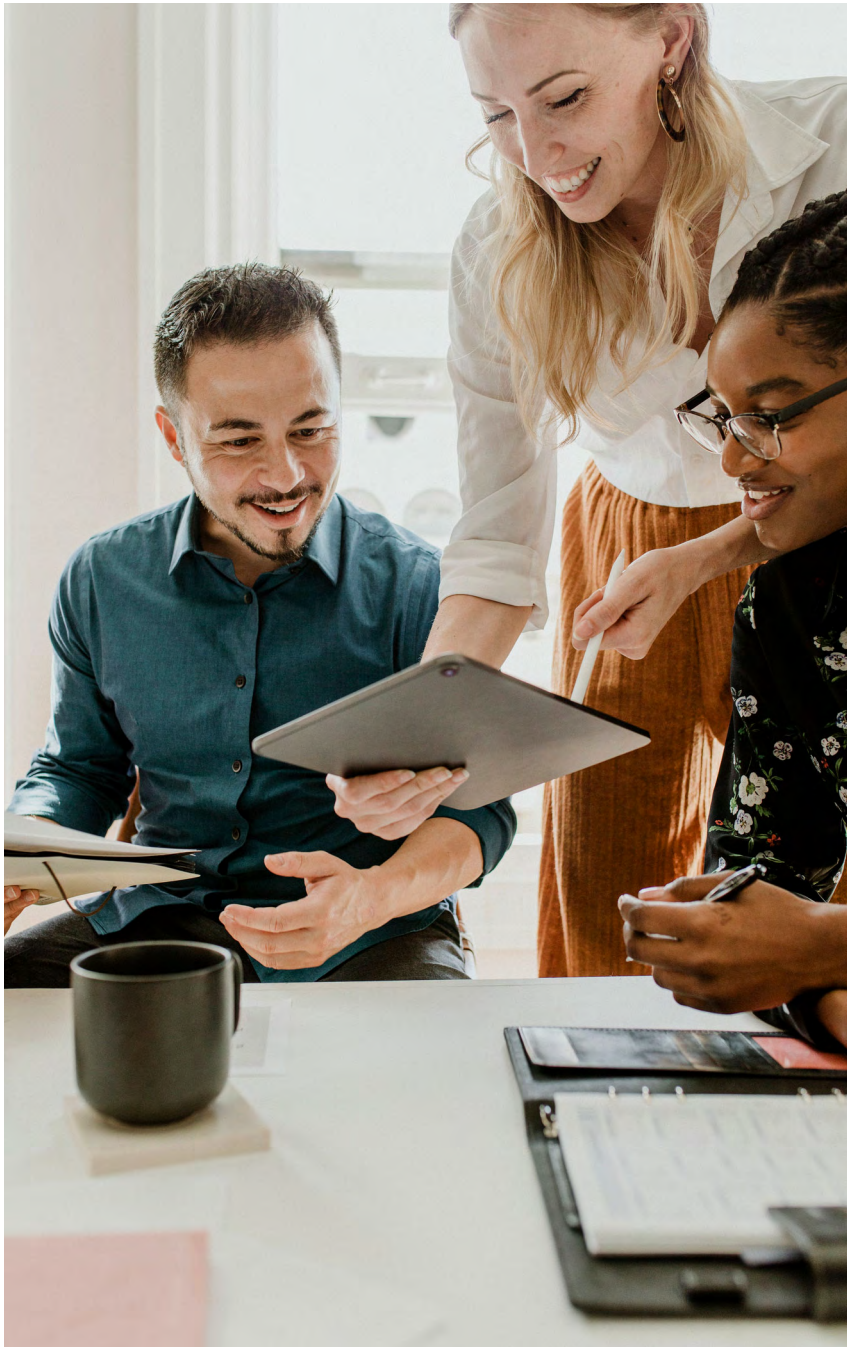
Vulnerability Assessment

Penetration Testing

360 CYBER ESSENTIAL
360 CYBER SHIELD
360 CYBER ADVANCED

360 CYBER ESSENTIAL

360 CYBER ESSENTIAL is an entry-level cybersecurity as a service and compliance program strategically crafted to cater to the needs of organizations across various industries, regardless of their current cybersecurity maturity level. Designed for companies lacking internal cybersecurity resources and seeking strategic guidance to bolster their security and compliance posture, 360 CYBER Essential offers a two–to three-year roadmap with annual deliverables tailored to address specific organizational requirements.



360 CYBER SHIELD

360 CYBER SHIELD is our mid-level cybersecurity and compliance program tailored for organizations seeking to mature their existing security programs. With a focus on enhancing security posture and ensuring regulatory compliance, 360 CYBER Shield is ideal for companies with some cybersecurity infrastructure but limited internal resources. Our cybersecurity as a service program offers strategic guidance, protection against evolving cyber threats, and support for compliance frameworks such as HITRUST, ISO 27001, PCI, HIPAA, or SOC. Let us empower your organization to navigate the complexities of cybersecurity with confidence and resilience.

360 CYBER ADVANCED

360 CYBER ADVANCED, our top-tier cybersecurity and compliance program, is designed to meet the needs of organizations looking to scale their existing security programs and enhance their cybersecurity posture. Tailored for companies with established security frameworks, 360 CYBER Advanced offers custom compliance program support and cybersecurity services to address specific organizational requirements. Additionally, our program provides executive-level support to communicate cybersecurity strategies and initiatives to key stakeholders effectively.

Let 360 CYBER Advanced be your trusted resources in advancing your cybersecurity capabilities and achieving your organizational goals.

360 CYBER MANAGED SERVICES

ESSENTIALS	SHIELD	ADVANCED
CLaaS – Cybersecurity Leadership as a Service	CLaaS – Cybersecurity Leadership as a Service	CLaaS – Cybersecurity Leadership as a Service
Periodic Executive Reporting & Presentation	Periodic Executive Reporting & Presentation	Periodic Executive Reporting & Presentation
Annual Gap or Risk Assessment	Annual Gap or Risk Assessment	Annual Gap or Risk Assessment
Audit Coordination & Facilitation	Audit Coordination & Facilitation	Audit Coordination & Facilitation
Policies & Procedures Development Assistance	Policies & Procedures Development Assistance	Policies & Procedures Development Assistance
Compliance Program Remediation Assistance	Compliance Program Remediation Assistance	Compliance Program Remediation Assistance
	GRC Platform Setup and Administration	GRC Platform Setup and Administration
	Annual Security Awareness Training	Annual Security Awareness Training
	Vendor Risk Management	Vendor Risk Management
	Customer Security Questionnaires	Customer Security Questionnaires
	Quarterly Vulnerability Scanning	Quarterly Vulnerability Scanning
		Annual Business Impact Analysis
		Annual Incident Response / Business Continuity / Disaster Recovery Tabletop Exercises
		Annual Penetration Testing
Starting at $4,000 per month*	**Starting at $6,000 per month***	**Starting at $10,000 per month***

**Assumes a low-complexity client*

360 CYBER MANAGED SERVICES

The table below describes some of the common factors that are used to determine the level of complexity associated with a managed services engagement. The complexity is used to determine the level of effort and associated fees for the engagement. The table is not intended to be all-inclusive.

CLIENT COMPLEXITY FACTORS			
ATTRIBUTES	LOW	MODERATE	HIGH
Company Profile	Start up or small business Annual revenue < $10M Less than 50 employees Single office location	Small or medium-sized business Annual revenue $10M - $50M 51 – 200 employees Multiple office locations	Large Enterprise business Annual revenue > $50M 51 – 200 employees Many & global mixed-use locations (office manufacturing, distribution, data center
Compliance Standards	SOC 2 Type 1 or Type 2 Common Criteria PCI SAQ-A, SAQ-B HITRUST e1 CMMC Level 1 HIPAA Security Rule	SOC 2 Type 2 All Criteria PCI SAQ-C, SAQ-D ISO 27001/2 HITRUST i1 CIS Critical Security Controls (IG 1 & 2) HIPAA Security and Privacy Rule	HITRUST r2 PCI-DSS Certification (i.e., ROC) NIST 800-171 / CMMC Level 2 and 3 FedRAMP / GovRAMP NIST 800-53 / FISMA
Technology	Single cloud service provider On-premises only infrastructure < 100 technology endpoints Few SaaS products Little or no application development	Hybrid infrastructure (cloud & on-premises) 101 – 1,000 technology endpoints Moderate # of SaaS products Minimal in-house or outsourced application and systems development	Multiple cloud service providers and/or hybrid infrastructure (cloud & on-premises) > 1,000 technology endpoints Several SaaS products Extensive in-house or outsourced application and systems development Many third-party dependencies

360 CYBER MANAGED SERVICES

SERVICES	DESCRIPTION OF SERVICE / DELIVERABLE
Cybersecurity Leadership as a Service (CLaaS)	**Description:** Provide strategic cybersecurity leadership and guidance, helping to develop and implement security policies, plans, standards, procedures, and programs. **Deliverable:** • Program Charter • Verbal and/or written guidance and recommendations
Periodic Status Reporting	**Description:** Meetings with management team to discuss progress, achievements and upcoming plans and initiatives. **Deliverable:** Periodic Status Reports
Periodic Executive Reporting & Presentation	**Description:** Summarizes key metrics such as risk management, compliance status, security incidents, and progress on initiatives. Highlights accomplishments, emerging threats, and any challenges while outlining upcoming priorities and potential resource needs. Delivered in a clear and concise format, these updates ensure that senior leadership stays informed and can make strategic decisions to strengthen the company's cybersecurity posture. **Deliverable:** Executive presentation and status update
Policies & Procedures Development Assistance	**Description:** Develop and/or maintain a set of cybersecurity-related [policies, plans, standards, and procedures] **Deliverable:** A set of cybersecurity-related [policies, plans, standards, and procedures], in accordance with the requirements set forth in [ADD STANDARD].
Security Questionnaire Assistance	**Description:** Perform review of customer security questionnaires to understand the customer's specific concerns and compliance requirements. Coordinate with internal teams to gather relevant documentation, such as policies, procedures, and certifications, and complete the questionnaire with precise details. Any gaps or areas of concern are addressed by explaining mitigation strategies or planned improvements. Before submission, the responses are reviewed for consistency and clarity. This process also identifies trends in customer inquiries, driving future enhancements to the organization's security practices. **Deliverable:** Completed questionnaires and cumulative inventory of past questions/topics & responses.
Audit Coordination & Facilitation	**Description:** Assistance in gathering artifacts requested by the auditor, such as logs, access records, and security configurations to ensure requests are fulfilled without unnecessary exposure. During applicable audits, assistance will be provided to address questions and ensure clarity. The process concludes with post-audit support, including responding to findings and providing guidance for improvements to enhance compliance. **Deliverable:** Verbal and/or written guidance and recommendations
Risk Assessment	**Description:** Risk assessment of IT environment using a custom NIST 800-30 based framework, evaluated against [ADD STANDARD] controls. This includes asset, threat, and vulnerability identification; impact and likelihood analysis; and risk level determination. A detailed report with prioritized risk mitigation recommendations will be provided. **Deliverable:** A detailed risk assessment report including a prioritized list of identified risks, recommendations for risk mitigation strategies, and an executive summary highlighting key findings and proposed actions.

360 CYBER MANAGED SERVICES

SERVICES	DESCRIPTION OF SERVICE / DELIVERABLE
Security Architecture Review	**Description:** Advise in developing the mechanisms for conducting [a one-time, as-needed] evaluation(s) of existing security infrastructure, policies, and practices aimed to identify strengths, weaknesses, and areas for improvement in the current security architecture and ensure it aligns with business objectives, industry best practices, and relevant regulatory requirements; as well as ensure the Security Architect is provided the support to improve on the overall security architecture structure. **Deliverable:** Verbal and/or written guidance and recommendations
Compliance Program Gap Assessment	**Description:** The Cybersecurity Program Gap Assessment service evaluates CLIENT's current cybersecurity program against the industry standard frameworks chosen and includes [ADD STANDARD]. The assessment identifies deficiencies in policies, technology, configurations, and processes, providing insight into areas needing improvement to achieve compliance or enhance the organization's security posture. Recommendations will be provided based on risk and impact. **Deliverable:** A cybersecurity compliance gap assessment report including an executive summary and risk-based recommendations.
Compliance Program Remediation Assistance	**Description:** The Cybersecurity Program Remediation Assistance service helps implement corrective actions to address gaps and vulnerabilities identified in previous assessments. The service focuses on strengthening security controls, processes, and policies to align with industry frameworks and changes to the IT environment during the duration of the SOW. Guidance and support will be provided throughout the remediation process, ensuring timely and effective improvements of security posture. **Deliverable:** · Remediation Action Plan · Implementation Support · Progress Tracking Reports
Security Awareness Training	**Description:** Training will be delivered through [interactive sessions, e-learning modules, and/or real-world simulations like phishing tests] to reinforce key lessons. Feedback and metrics are collected to measure effectiveness and address gaps. Regular updates ensure the training reflects emerging threats and compliance requirements, fostering a culture of continuous awareness and proactive security behavior. **Deliverable:** [Select all that apply] · Training Plan · E-Learning Modules · Interactive Session Materials · Phishing Simulation Reports · Participant Completion Records · Training Effectiveness Metrics · Updated Training Content · Threat Awareness Bulletins · Compliance Tracking Documentation

360 CYBER MANAGED SERVICES

SERVICES	DESCRIPTION OF SERVICE / DELIVERABLE
Internal Audit Services	**Description:** Perform an annual independent internal audit of the XXX program and identify gaps/non-conformities and opportunities for improvement **Deliverable:** Internal Audit Report in accordance with XXX requirements
GRC Platform Setup & Administration	**Description:** Implement and maintain the GRC platform **Deliverable:** Implemented and configured GRC platform
Third Party Risk Management	**Description:** Track and categorize vendors based on their access to sensitive data or systems. Security requirements are defined, vendor documentation such as SOC reports or certifications are reviewed, and risk assessments and/or security questionnaires are conducted. Identified risks are addressed through remediation plans, contract updates, or additional controls. Regular monitoring, including periodic reassessments and performance reviews, ensures vendors maintain compliance. **Deliverable:** Vendor Inventory, Vendor Due Diligence Questionnaire (lite and/or full assessment), Vendor Due Diligence Assessment Reports
Customer Contract Review	**Description:** Review and provide formal feedback related to any cybersecurity clauses and requirements. **Deliverables:** Verbal and/or written guidance and recommendations
Tabletop Exercises	**Description:** Tabletop exercises will be conducted to simulate incident response and disaster recovery scenarios, testing the organization's preparedness and response capabilities. These exercises will involve key stakeholders from various departments and will follow a structured approach to simulate real-world incidents, such as cyberattacks, data breaches, or system outages. The exercises will focus on decision-making, communication, and coordination among teams. **Deliverable:** A detailed report will be provided, summarizing the exercise, identifying gaps in the response, and offering recommendations for improvement.
Vulnerability Scanning	**Description:** Vulnerability scanning helps organizations identify, assess, and prioritize security vulnerabilities within their IT environment and involves using automated tools to scan networks, systems, applications, and devices for known weaknesses, misconfigurations, and outdated software. **Deliverable:** A detailed vulnerability scan report is generated that outlines the findings and provides actionable recommendations for remediation. Vulnerability scanning will be performed [as a one-time assessment or on an ongoing basis].
Penetration Testing	**Description:** Penetration testing will involve simulating cyberattacks to identify vulnerabilities in external and internal networks, web applications, and cloud infrastructure. Certified testers will follow industry-standard methodologies, including reconnaissance, vulnerability analysis, exploitation, and post-exploitation, to assess security posture. **Deliverable:** A report will be provided, detailing identified vulnerabilities, their potential impact, and prioritized remediation recommendations. An executive summary for senior management and a follow-up test to validate remediation efforts (if needed) may also be included. All testing will adhere to CLIENT's security policies and compliance requirements.

SUPPORT SERVICES PORTFOLIO

PRIVACY

CALIFORNIA CONSUMER PRIVACY ACT

GDPR

NETWORK SECURITY

PENETRATION TESTED
PEN TESTED
SERVICE ORGANIZATION
TESTING PERFORMED BY 360 ADVANCED

COMPLIANCE

SOX COMPLIANCE

HIPAA

AICPA SOC
aicpa.org/soc4so

ISO

HITRUST

CSA STAR

PCI DSS

NIST

GOVERNMENT

FedRAMP

GovRAMP

FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT

CYBERSECURITY MATURITY MODEL
CERTIFICATION
CENTER OF EXCELLENCE

GLBA
FISMA
SOX

360ADVANCED

Let's Connect

Contact

866-418-1708