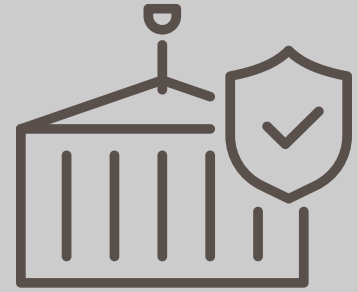# ORBITALFIRE
CYBERSECURITY

SERVICE OVERVIEW

COMPLIANCE ASSESSMENT

Our Compliance Assessment service provides comprehensive analysis of all in-scope cybersecurity controls, ensuring complete understanding of compliance and risks.

BENEFITS

o   Identified Critical Cybersecurity Risks

o   Optimized Cybersecurity Investments
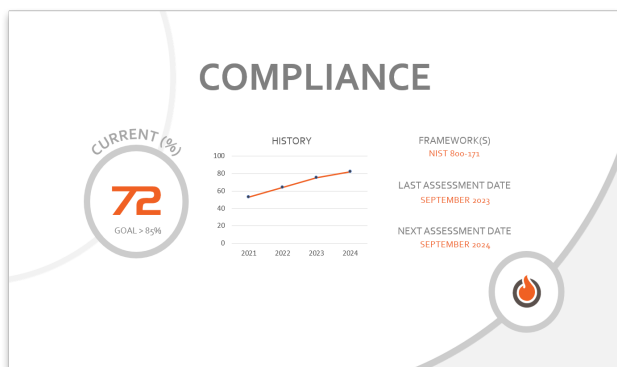
o   Improved Regulatory Compliance

FRAMEWORKS

Framework expertise includes:

CMMC, DFARS, NIST 171, HIPAA, NYSDFS, PCI, FTC SAFEGUARDS, SEC

FEATURES

o   Expert-led controls evaluation for all in-scope cybersecurity controls.

o   Comprehensive Findings documentation, including summary and detailed control-by-control scoring.

o   Detailed, risk-based recommendations.

o   Integrated compliance and risk assessment in a single effort.

COMPLIANCE

CURRENT (%)

72

GOAL > 85%

HISTORY

100
80
60
40
20
0

2021 2022 2023 2024

FRAMEWORK(S)
NIST 800-171

LAST ASSESSMENT DATE
SEPTEMBER 2023

NEXT ASSESSMENT DATE
SEPTEMBER 2024

ORBITALFIRE
CYBERSECURITY

AFFORDABLE, OUTSOURCED
CYBERSECURITY
SERVICES FOR SMALL BUSINESSES

REGULATORY COMLPIANCE
Compliance expertise across industries, including Manufacturing, Healthcare, Finance, Auto, and more.

INTRUSION & THREAT DETECTION
24x7 automated detection of threats, intrusions, and other malicious activity.

AWARENESS TRAINING
Continuous and automated employee training, education, and newsletters.

VULNERABILITY MANAGEMENT
Automated scanning of computers, servers and devices for vulnerabilities.

COMPREHENSIVE ASSESSMENTS
Comprehensive evaluation of your security posture, policies, procedures, and systems.

CLOUD SECURITY
Secure your most critical assets in the cloud, including Office 365.

VIRTUAL CISO
Guidance and assistance with all things cybersecurity.

POLICY & PLAN DEVELOPMENT
Comprehensive strategy development to strengthen security and protect against potential threats.

INCIDENT RESPONSE TABLETOP
Test and assess your Incident Response capability in a realistic, safe, and controlled environment.

INCIDENT RESPONSE
Advanced investigative services during cybersecurity events .

PENETRATION TESTING
Realistic but safe simulation of cybercriminal attacks.

CONFIGURATION MANAGEMENT
Regular, automated scanning of computers, servers and devices for configuration errors and weaknesses.

DARK WEB BREACH DETECTION
Automated detection of threats, intrusions, hacking, and other malicious activity.