THRIVE℠

Cybersecurity Risk Assessment

Evidence-based evaluation and strategic planning of organizational cybersecurity posture

Thrive's Cybersecurity Risk Assessments evaluate cybersecurity posture and risk mitigation tools against the Center for Internet Security's (CIS) 18 control areas to provide a comprehensive picture of the client's current risk profile while developing a strategic roadmap for the future.

- Thrive's consultants are (ISC)² certified trusted advisors
- Review of existing policies, controls, and compliance oversight
- Center for Internet Security (CIS) framework implementation
- Information security governance and compliance oversight
- Third-party partner due diligence initiatives
- Evidence based assessment provides true cybersecurity strategy validation
- Provide executive level reporting on the organizations risk profile
- Provide a prioritized roadmap for weakness mitigation
- Deliver tailored prescriptive remediation advice as required

CIS Center for Internet Security® NIST CYBER ESSENTIALS

Meeting Cyber Essentials requirements and more closely aligning with NIST standards through CIS.

(continued)

"Thrive's approach was not just about ticking boxes; it was about **truly understanding our security posture and helping us navigate the complexities of cybersecurity in our industry.** Their partnership has been instrumental in affirming our security foundations and identifying areas for improvement."

David Boulton, *IT Manager at Zeus Capital*

3 Steps to Cybersecurity Risk Assessment

1) Current State Overview

Thrive first looks under the hood to assess everything your organization has at play. An CRA oftentimes requires delegate access to your organization's existing systems, and even a visit to your offices to check out any on-premise equipment and endpoint devices. During the assessment, Thrive's team reviews all three levels of controls (18) – basic, foundational, and organizational.

2) CIS Comparison

After assessing where your organization stands on each of the 18 CIS v8 controls, Thrive compares its findings with recommended best practices. These best practices include NextGen firewalling, overarching governance plans, and multifactor authentication (MFA) usage across logins. This gap analysis compares your organization's properly deployed protocols against those typically prescribed to improve security posture.

3) Prioritized List

As a final step during your CRA, Thrive prepares and presents a clear report that is built for both executives and tech teams alike. This review recaps the CIS standards and presents them in an easy-to-read table, comparing your security posture with the most up-to-date mitigation tactics. Each area of non-compliance is then flagged with an associated level of urgency – low, medium, or high. Along with these recommendations, Thrive gives your team an approximate associated cost on the open market to bring your security position into compliance.

Summary

In today's ever evolving IT landscape, the CRA provides organizations with the insight into the largest risks their business face today. The assessment is cost effective, light touch and is based solely on providing you with a clear view of your current cybersecurity state and actionable outcomes to improve your overall cybersecurity posture.

About Thrive

Thrive delivers global technology outsourcing for cybersecurity, Cloud, networking, and other complex IT requirements. Thrive's NextGen platform enables customers to increase business efficiencies through standardization, scalability, and automation, delivering oversized technology returns on investment (ROI). They accomplish this with advisory services, vCISO, vCIO, consulting, project implementation, solution architects, and a best-in-class subscription-based technology platform. Thrive delivers exceptional high-touch service through its POD approach of subject matter experts and global 24x7x365 SOC, NOC, and centralized services teams. Learn more at **www.thrivenextgen.com** or follow us on **LinkedIn**.