Why cStor for Your Cybersecurity Framework Gap Analysis?

The cStor Cybersecurity Framework Gap Analysis is an important step towards creating a prioritized, risk-based roadmap to improve the cybersecurity posture of an organization. By making an objective examination of the cybersecurity environment, organizations gain valuable insight into the current state and are provided with the information needed to move to a more protected state.

This Gap Analysis will cover either the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) or the Center for Internet Security's (CIS) Controls framework.

SERVICE SIZE AND PRICING

The cStor Cybersecurity Framework Gap Analysis service is sized and priced based on the following criteria:

SIZE	EMPLOYEES	LOCATIONS	APPLICATIONS
Small	0 to 50	1	less than 3 critical applications to review
Medium	51-250	2 to 3	4 to 6 critical applications to review
Large	251-1000	4 to 5	7 to 10 critical applications to review
Extra Large	1001-2500	5 to 6	10 to 15 critical applications to review

A cStor Project Manager will ensure the project delivers successfully and as outlined in this Service Brief.

Service Feature Highlights

cStor Cybersecurity Framework Gap Analysis is an independent review conducted by a cStor third-party contractor that is designed to examine the client environment and compare the current state to each of the controls defined in their chosen Cybersecurity Framework. A final report, detailing the findings of the review is provided by the contractor.

SERVICE FEATURES

During the engagement, a contractor consultant will visit the client site to conduct the analysis. This is typically done in-person; however, the assessment can be completed remotely if an in-person assessment is impractical or otherwise precluded for the health and safety of those involved.

Through a detailed series of interviews and observations, the consultant will document the current state of the environment as compared to each of the 108 controls in the NIST CSF or the 171 controls in the CIS Controls. These findings will be thoroughly documented in a final report that also provides recommendations and highlights any critical weaknesses identified.

cStor
We look beyond IT

While the assessment and report are completed by the contractor, cStor will provide project management and quality assurance services to ensure the project is completed in a timely manner and provides high-value deliverables.

A cStor security engineer will import data from the final report from the contractor into a cStor proprietary dashboard to allow the client to visualize the results and prioritize future actions. A cStor security engineer will also use information from the report to create a suggested roadmap and present this roadmap as a PowerPoint presentation in a strategic planning meeting held with the client at a time mutually agreeable to cStor and the client, typically about two (2) weeks after the consultant has presented their report to the client.

Responsibilities

CONTRACTOR RESPONSIBILITIES

- Perform a Gap Analysis utilizing the appropriate control set.
- Produce a Gap Analysis Report that compares the baseline technical controls in place today to the control requirements.
- Develop recommendations that can be used as a guide to remediate control gaps.

CSTOR RESPONSIBILITIES

- Provide Project Management services to oversee the completion of the project.
- Review consultant deliverables and provide feedback as needed to improve quality.
- Populate the cStor Scorecard Tool with client data from the assessment and deliver a PDF copy of the Scorecard's Dashboard to the client.
- Create a proposed cybersecurity roadmap and deliver it to the client as a PowerPoint presentation in a strategic planning meeting.

CLIENT RESPONSIBILITIES

- Contact a cStor project manager to schedule and provide for the delivery of the service within 90 days of purchase.
- Provide a designated point of contact (POC) to facilitate access to information, systems, and individuals required to perform the services. Ideally, the POC will have system and network administration skills.
- Adherence to all cStor's services terms and conditions located at www.cstor.com/legal.
- Clients must provide at least two (2) weeks of advanced notice to schedule service delivery.

SHARED RESPONSIBILITIES

- The entire cStor service must be completed within twelve (12) months of the engagement start date. Otherwise, the order will be automatically terminated and deemed complete.
- cStor will send the client a confirmation email when the service is complete, providing an opportunity for the client to advise if the service was not delivered satisfactorily. If the client does not submit a written notification of a service performance issue within five (5) business days from receipt of the confirmation email, the work will be deemed accepted.

cStor
We look beyond IT

Exclusions

The following items are not included in the Cybersecurity Framework Gap Analysis:

- Any services not listed earlier.

Other deviations from service scope can be accommodated with the purchase of additional cStor services. Activities are delivered during cStor local standard business hours unless additional services have been purchased or special arrangements have been made.

Fee Description and Payment

Before the performance of any services, cStor requires an approved purchase order from the client, acceptable to cStor. cStor may invoice upon receipt of the approved purchase order. Payments are non-refundable with no right to refund or credit. If the client requires additional services time, a new cStor sales quote and purchase order will be required.

Additional Services

By completing a Cybersecurity Gap Analysis and Strategic Roadmap, the client has taken a significant step towards improving their security posture. To help our clients continue that forward momentum, cStor offers a ManageWise for Gap Analysis service. With this service, cStor engineers meet with our clients on a regular cadence to discuss the changes implemented in their environment than then use that information to update the Scorecard Tool and deliver a new PDF copy of the Dashboard that can be used to illustrate the progress made since the last update. For more details, ask your cStor Account Manager for a ManageWise for Gap Analysis Service Brief.

cStor can assist in every phase of the cybersecurity lifecycle. Whether help is needed in planning a next-generation solution, an extra set of hands for a major deployment or strategizing for optimizing an existing security infrastructure, cStor service personnel have the skills to help clients start it right and keep it right. cStor offers a complete portfolio of related services, including consulting, design, implementation and support services.

The Gap Analysis gives you a starting point, helping you determine where you need to focus to build out your short- and long-term plans.

BENEFITS OF A CSTOR CYBERSECURITY FRAMEWORK GAP ANALYSIS

1 ### Expert Resources
Outsourcing your Gap Analysis ensures you have a skilled team to provide you with an open, unbiased view of your environment.

2 ### Fast Results
With years of expertise and a proven process, cStor reduces the delivery time from months to weeks.

3 ### Comprehensive Scope
cStor's Gap Analysis includes as much of the environment as possible to ensure proper coverage while trimming out unnecessary areas and duplication to optimize your budget.

4 ### Proven Methodologies
The Gap Analysis includes a combination of inquiry, observation and verification/testing to ensure you receive an accurate measure of your risk and in-depth analysis unique to your environment.

5 ### Actionable Intelligence
cStor provides you with a skilled partner experienced in delivering quality, actionable results.

Let's Get Started

Learn more about how cStor can work with your team to capitalize on today's leading technologies and maximize your IT investments. Contact your cStor Account Executive or Solutions Architect to schedule a consultation today.

cStor
We look beyond IT

info@cStor.com
www.cStor.com
877-CSTOR-81
(278-6781)