Cybersecurity Compliance Readiness Assessment

Introduction

To help implement higher cybersecurity safeguarding standards across the industry, the Department of Defense (DoD) has announced the adoption of a new set of cybersecurity controls. These requirements are captured in Defense Federal Acquisition Regulation Supplement (DFARS) provision 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting." Controls are derived from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Security and Privacy Controls for Non-Federal Information Systems," which was developed and released by NIST with the intention of providing contractors with standards and requirements more appropriate for non-government organizations.

What does all of this mean for defense contractors and their entire supply chains?

- They must fully understand what covered defense information (CDI) is and whether they store, process, or transmit CDI in the course of doing business with DoD.
- They must meet the 110 security control requirements identified in NIST SP 800-171.
- They must report any shortcomings or gaps to the DoD's Chief Information Officer (CIO) within 30 days of any contract award.
- They must implement all NIST SP 800-171 controls by December 31, 2017.

This makes performing a compliance assessment a top priority for defense contractors and their supply chains. Failure to do so can jeopardize current contracts and future contract awards.

A compliance assessment requires time, resources, cybersecurity expertise, and an intimate understanding of the NIST SP 800-171 security controls. For these reasons, organizations may choose to have a qualified, independent party support their team when conducting the analysis.

What is a Cybersecurity Compliance Readiness Assessment?

A Cybersecurity Compliance Readiness Assessment (CCRA) consists of three activities performed by an assessment team:

- *Gathering data* to understand an organization's current security posture.
- *Evaluating data* to measure the effectiveness of security controls and identify gaps in the performance of these controls with respect to a security framework (in this case, NIST SP 800-171).
- *Developing recommendations* to create the required reporting documentation for the DoD CIO and the roadmap and action plan to address shortcomings.

Discovery

Data Gathering and Evaluation

The assessment team will review documentation provided by the organization about its IT environment, including key policies, procedures, processes, and any other relevant information. The assessment will also involve interviews with personnel responsible for cybersecurity governance (e.g., IT, security, HR, legal, etc.), as well as information system users with access to CDI. The primary goal of these activities is to verify the existence of controls and determine whether they are in alignment with the standards set forth in NIST SP 800-171. Any deficiencies will be noted as gaps.

Recommendations Requirements

The assessment team will produce a compliance assessment report. The report will identify gaps that exist between the performance of an organization's security control and an effective, compliant control in objective, clear, and understandable terms. It will define what constitutes the gap, the factors that contribute to it, and its priority. The report also will include options to address the shortcoming, along with a recommended plan of action that serves as the basis for a strategic roadmap and a tactical implementation plan (Enterprise Strategic Plan, or ESP).

Exostar's Cybersecurity Compliance Readiness Assessment Service

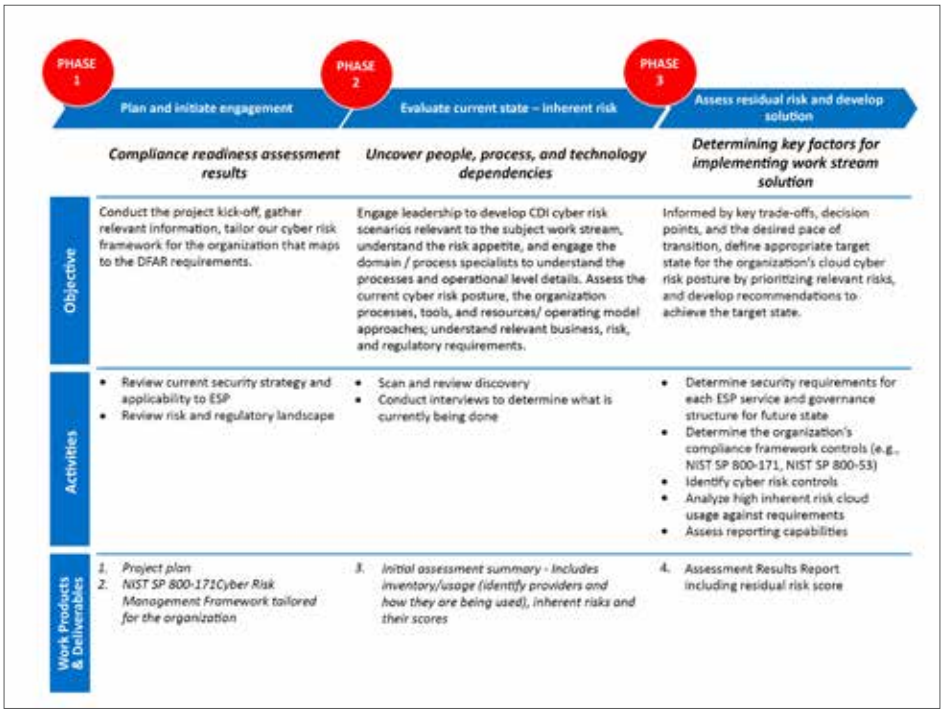
Exostar offers a professional service to assess a defense organization's information security controls specifically as they relate to the NIST SP 800-171 controls. This service arms contractors with the information and documentation they need to demonstrate DFARS 252.204-7012 compliance and meet its reporting requirements.

The Cybersecurity Compliance Readiness Assessment is administered by a top-tier, certified cybersecurity professional team that examines the performance of all 109 NIST SP 800-171 security controls, as well as other defense industry security requirements and current best practices.

The team identifies any gaps in performance or coverage of the controls and provides recommendations for remediation, which are included in a plan of action and remediation roadmap. The resulting report can be used not only in conjunction with DoD reporting requirements, but also as a benchmark and plan for continuing improvement of the organization's security posture.

Why Exostar

For nearly two decades, Exostar has been helping organizations in highly-regulated industries mitigate risk, solve identity and access challenges, and collaborate securely across their supply chain ecosystems. By offering connect-once, collect-once, certify-once access to partners, Exostar's solutions strengthen security, reduce expenditures, and raise productivity so organizations can better meet contractual, regulatory, and time-to-market objectives. These solutions are used today by 98 of the top 100 global aerospace and defense companies.



Contact Exostar Today | sales@exostar.com | 703.793.7733

About Exostar

Exostar's cloud-based solutions help companies in highly-regulated industries mitigate risk and solve identity and access challenges. Nearly 125,000 organizations leverage Exostar to help them collaborate securely, efficiently, and compliantly with their partners and suppliers. By offering connect-once, single sign-on access, Exostar strengthens security, reduces expenditures, and raises productivity so customers can better meet contractual, regulatory, and time-to-market objectives.