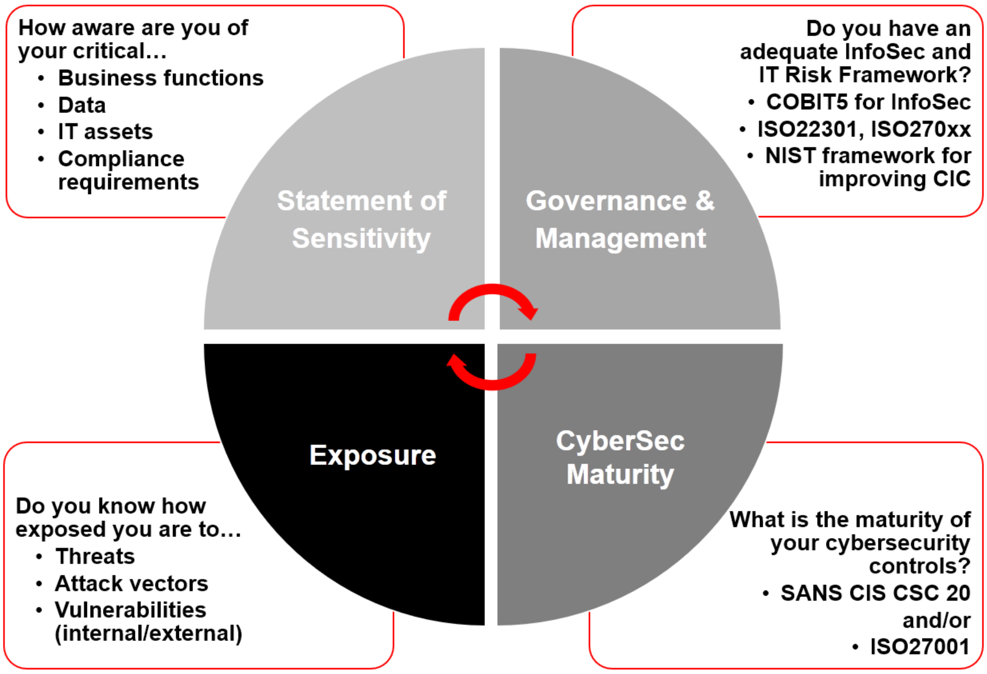
CYBERSECURITY POSTURE ASSESSMENT

What is a Cybersecurity Posture Assessment?

Based on the definition by the National Institute of Standards and Technology (NIST), the term *security posture* refers to the security status of an enterprise's hardware, software and policies, its capability to manage its defenses and its ability to react as the situation changes. A Cybersecurity Posture Assessment provides an overview of a customer's internal and external security posture by integrating all the facets of security into the same assessment approach. It provides an overall answer to the following questions:



How aware are you of your critical…
- Business functions
- Data
- IT assets
- Compliance requirements

Do you have an adequate InfoSec and IT Risk Framework?
- COBIT5 for InfoSec
- ISO22301, ISO270xx
- NIST framework for improving CIC

Do you know how exposed you are to…
- Threats
- Attack vectors
- Vulnerabilities (internal/external)

What is the maturity of your cybersecurity controls?
- SANS CIS CSC 20 and/or
- ISO27001

The 4 Key Elements of a Cybersecurity Posture Assessment

Hitachi Systems Security's Cybersecurity Posture Assessment relies on a variety of existing standards, guidelines, and practices to enable your critical infrastructure to achieve resilience. By reviewing how critical assets are managed and their associated security controls, including your security policies and processes framework, by performing a threat and risk review and addressing any gaps found during the assessment, the Cybersecurity Posture Assessment will help design and develop an appropriate cybersecurity roadmap within an overall security program and business continuity planning.

Objectives

Our Cybersecurity Posture Assessments have been designed to help your organization:

- Assess the strengths and weaknesses of your cybersecurity posture
- Ensure that appropriate measures are in place to protect the confidentiality, integrity and availability of your critical information and assets under the assessment
- Help you define a clear path going forward in your cybersecurity planning
- Provide you with relevant information necessary to strengthen your cybersecurity position and advise you of solutions to protect your business going forward

BENEFITS

- ► Know your cybersecurity posture
- ► Understand where you are, where you need to go and what needs to be done to get there
- ► Facilitate targeted spending on safeguards to fortify your cybersecurity posture
- ► Gain deeper knowledge of vulnerabilities and threats through proactive risk management
- ► Build a bridge between enterprise risk management and operational security efficiency

Elements of a Cybersecurity Posture Assessment

✓✓ Phase 1: Planning and Preparation

The first step is a thorough planning exercise. This is required before initiating a Cybersecurity Posture Assessment to validate the scope of the assessment, identify key stakeholders, identify resource requirements and finally, develop a realistic work plan.

To achieve these goals, a Hitachi Systems Security Project Manager will work in close cooperation with the appropriate stakeholders at the client organization to develop a detailed work plan, including a clearly-stated aim, a statement of scope, limitations and restrictions, required logistical arrangements, a detailed schedule and deliverables.

✓✓ Phase 2: Documentation Review

To prepare the other phases, Hitachi Systems Security will be provided with all reference material required, and any other information necessary for the completion of these tasks. To do so, a system description is documented, and a concept of operation is defined. Target level of residual risk is determined in consultation with the Client.

In this phase, Hitachi Systems Security will conduct a complete review of documentation including but not limited to information security policies, processes and procedures, critical business processes, risk management plans, network diagrams, security architecture etc.

✓✓ Phase 3: Assessment

During the assessment phase, our team of consultants will conduct an analysis of the client’s internet exposure, conduct an onsite audit followed by an analysis of findings, define the overall cybersecurity posture of the client based on these findings and results and propose a prioritized improvement plan including suitable recommendations for the security authority.

✓✓ Phase 4: Reporting

Upon completion of the Cybersecurity Posture Assessment, a draft report will be sent to the client, including all the above-identified deliverables. Once the comments will have been received and integrated, Hitachi Systems Security will provide the client with the final report.

WANT TO LEARN MORE?

Contact us at info@hitachi-systems-security.com

in You Tube