



**TechForce<sup>™</sup>  
Cyber**

# **Cyber Security Maturity Assessment Service Definition**



## Service Overview

- **Description:** The Cyber Security Maturity Assessment service provides an in-depth evaluation of an organization's cyber security posture, identifying strengths, weaknesses, and areas for improvement across all cyber security operations. The service is designed to benchmark your organization's cyber security measures against industry standards and best practices.
- **Objective:** To help organizations enhance their resilience against cyber threats by providing a clear and actionable roadmap to improve their security stance.

## 2. Service Features

- **Comprehensive Assessment:** Evaluate current cyber security practices, policies, and procedures.
- **Risk Identification:** Identify vulnerabilities and threats specific to the organization.
- **Maturity Scoring:** Rank cyber security practices according to maturity levels to understand current capabilities.
- **Benchmarks Against Standards:** Use established frameworks like NIST, ISO/IEC 27001, and others for benchmarking.
- **Customized Reporting:** Provide detailed reports with findings, implications, and recommendations.
- **Actionable Insights:** Offer strategic and tactical recommendations for improvements.
- **Follow-Up Reviews:** Scheduled follow-up assessments to monitor progress and update strategies.

## 3. Benefits

- **Enhanced Security Posture:** Strengthen defenses by closing gaps identified in the assessment.
- **Compliance and Alignment:** Ensure alignment with industry regulations and standards.
- **Strategic Planning:** Facilitate informed decision-making and strategic planning in cyber security investments.
- **Stakeholder Confidence:** Increase confidence among stakeholders with verified security measures.

## 4. Target Audience

- **Public Sector Organizations:** Designed specifically for government entities needing to assess and improve their cyber security maturity in accordance with public sector standards and requirements.
- **IT Departments and Security Teams:** Provide IT departments and security teams with insights and recommendations tailored to enhance their security operations.

## 5. Service Scope

- **Initial Consultation:** Understand client needs and customize the assessment scope.
- **Data Collection:** Gather data through surveys, interviews, and system analysis.
- **Analysis and Evaluation:** Analyze the collected data to assess the maturity levels and identify risks.
- **Reporting and Presentation:** Deliver a detailed report and present findings to the client's key stakeholders.
- **Follow-Up:** Offer options for periodic reassessment and consultation for ongoing improvement.



## 6. Service Deliverables

- **Assessment Report:** A comprehensive document detailing findings, risk analysis, and recommendations.
- **Executive Summary:** A high-level overview suitable for executive leadership.
- **Improvement Roadmap:** A prioritized list of recommended actions for improving maturity.

## 7. Assumptions and Dependencies

- **Access Requirements:** Client must provide necessary access to facilities, systems, and personnel.
- **Stakeholder Availability:** Timely availability of client's team members for interviews and discussions.
- **Regulatory Compliance:** The service will adhere to all applicable laws and regulations concerning data protection and privacy.

## 8. Pricing Model

- **Fixed Price:** Offered as a fixed-price service, based on the scope and scale of the assessment.
- **Customizable Add-ons:** Additional services available at predefined costs.

## 9. Terms and Conditions

- **Confidentiality:** All client data will be treated with strict confidentiality.
- **Data Protection:** Comply with GDPR and other relevant data protection regulations.
- **Service Agreement:** Details of the service level agreement (SLA) including delivery timelines, responsibilities, and warranties.



**TechForce™**  
**Cyber**