

CRITICALSTART®

Cybersecurity Readiness Assessment

KEY BENEFITS

- ✓ Improve your security architecture, tools and processes
- ✓ Enhance your cyber resilience

Evaluate all aspects of your cyber defense operations.

When it comes to cybersecurity preparedness, what you don't know can hurt you. Our Cybersecurity Readiness Assessment offerings utilize questionnaires, meetings and other methodologies to help you gauge your current operations and pinpoint opportunities for improvement.

You can choose from the following services, depending on your specific concerns:

YOUR CONCERNS	HOW WE CAN HELP	EXPECTED OUTCOMES
<p>Is my team ready to identify, respond to and recover from specific threat vectors, such as ransomware, business email compromise or insider threats?</p>	<p>Situational Readiness Assessments compare your technological, operational and governance landscapes against security best practices and well-known industry frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to identify strengths and weaknesses in your environment with respect to the chosen threat situation.</p>	<ul style="list-style-type: none"> ✓ Targeted qualitative maturity measurement against the five categories of the NIST CSF ✓ Short-term and long-term action plans for improving your security posture with respect to the chosen situation
<p>How does our implementation of existing technologies and processes compare to security best practices and industry standards?</p>	<p>Tactical Security Reviews measure your implementation of existing technologies and processes against security best practices and well-known industry frameworks such as the NIST CSF. These assessments are detailed reviews of settings, configurations and policy language to identify gaps between current state and applicable standards.</p>	<ul style="list-style-type: none"> ✓ List of recommendations for implementing changes in your environment, prioritized based on ease of implementation and criticality of deficiencies, with easier and/or more critical issues being addressed first ✓ Details on how to implement those changes, with focus on minimizing capital outlay for changes in favor of optimizing your use of existing solutions
<p>Is my team prepared to identify, respond to and recover from known and unknown security threats?</p>	<p>Strategic Security Assessments compare your technological, operational and governance landscapes against security best practices and well-known industry frameworks such as the NIST CSF to identify strengths and weaknesses in your environment.</p>	<ul style="list-style-type: none"> ✓ Comprehensive qualitative maturity measurement against the five categories of the NIST CSF ✓ Security roadmap for short-term and long-term improvements to your overall security posture