Solution Brief

BlueVoyant's CIS-Based Security Maturity Workshop

Illuminate the value of a maturity-based, holistic cyber program over individual service investments.

How effective is your security program?

Organizations have more cybersecurity tools than ever before, many of which overlap in functionality, leading to increased and unnecessary spending. Instead of aiming single products or services at individual pain points as they arise, a holistic solution is key.

The BlueVoyant CIS-based Security Maturity Workshop, led by a Proactive Services team member, illuminates the key elements to a holistic security program and helps identify your organization's strengths and vulnerabilities. Our maturity program is informed by the Center for Internet Security (CIS) Critical Security Controls and our own proprietary gap assessment methodology.

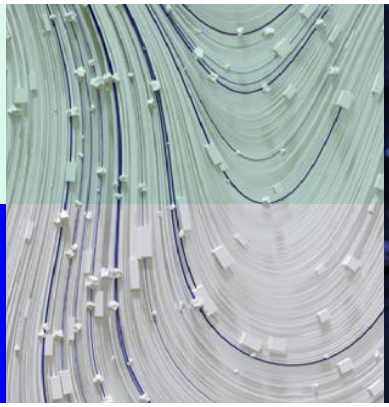
Do you have the appropriate cybersecurity people, processes, and technologies in place to ensure a holistic security program? If not, do you have a roadmap to help you achieve your desired state?

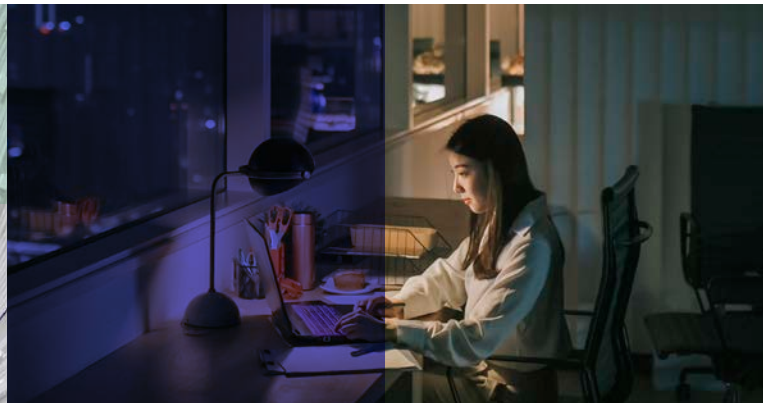
BlueVoyant's CIS-Based Security Maturity Workshop includes four phases: a brief overview of where we have been and where we are headed in cybersecurity; illustrations of how various factors influence risk; a review of our expert approach to identifying key cyber strengths and vulnerabilities; and an exercise to clarify your strengths and vulnerabilities, resulting in a findings and recommendations report.

Key Differentiators

- Maturity-based, holistic cybersecurity program based on CIS Controls v8 to provide you with a right-sized, integrated approach to improving your security posture.
- Our maturity model approach combines BlueVoyant's tailored risk-based assessment (People, Process, Technology, and Governance) with CIS IG Levels to eliminate the confusion associated with a "one-size-fits-all" framework that may be inadequate for complex organizations, or overwhelming to companies with limited resources.
- Our highly experienced team helps you understand the strengths and vulnerabilities in your overall security plan and then develops recommendations based on our proprietary methods layered onto the CIS v8 Implementation Group Controls.
- Our Liquid: PS™ consultants have extensive public and private sector frontline experience in responding to advanced cyber threats.

BlueVoyant





BlueVoyant's CIS-Based Security Maturity Workshop Phases

Information gathering
Prior to the workshop, BlueVoyant will send your organization a survey to collect some essential, non-proprietary data to conduct basic cybersecurity risk analysis and tailor the workshop to the client's particular circumstances.

Baseline current state vs. ideal state
Using results from the survey and discussion, BlueVoyant will lead an exercise designed to clarify the client's strengths and vulnerabilities, factoring in existing investments and practices. A high-level understanding of the client's security maturity is the goal of this exercise.

Right-sized cybersecurity discussion
The team will discuss lessons learned in building a robust cybersecurity program, best practices for right-sized cybersecurity investment, and how a maturity-based approach eliminates confusion — on where to start, how to measure success, and ensures orchestration among different security elements within the program.

Recommendations
The workshop will conclude with a review of recommendations for both gap remediation and target levels based on the content and output of the workshop, following the BlueVoyant methodology and the CIS v8 Implementation Groups.

Build common understanding
Illustrate how various circumstances influence risk, discuss the factors present in the client's environment, and build high-level consensus on organizational maturity level.

Remediation
Should you need help with remediating any gaps in your program, BlueVoyant's integrated team of professionals are prepared to help you reach and maintain your ideal security maturity.

Ready to learn more? Get in touch at contact@bluevoyant.com

BlueVoyant converges internal and external cyber defense capabilities into an outcomes-based, cloud-native platform called BlueVoyant Elements™. Elements continuously monitors your network, endpoints, attack surface, and supply chain as well as the open, deep, and dark web for vulnerabilities, risks, and threats; and takes action to protect your business, leveraging both machine learning-driven automation and human-led expertise. Elements can be deployed as independent solutions or together as a full-spectrum cyber defense platform. BlueVoyant's approach to cyber defense revolves around three key pillars — technology, telemetry, and talent — that deliver rock-solid cyber defense capabilities to more than 700 customers across the globe.

BlueVoyant

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com**