



Cybersecurity Risk Assessment

Safeguard your business reputation from security threats

Today's IT leaders must manage cybersecurity risks without impacting business growth. Blue Mantis Cybersecurity Risk Assessment solutions analyze the gaps in your current security posture.

Our assessments follow NIST, ISO 27001, PCI, HIPAA, SOC 2, CMMC, and other top security frameworks. Our experts conduct ransomware tabletop exercises, pen tests using the Penetration Testing Execution Standard (PTES), and more to develop a 360° view of the vulnerabilities and compliance lapses internal IT teams often miss.

Attain security maturity

Based on your desired business outcomes and budget, Blue Mantis can either provide an actionable incident response plan for your IT team to manage or partner with you to integrate our dedicated incident response and Security Operations Center (SOC) into your business processes for continuous monitoring and management of your cybersecurity risks.

See how you map to NIST Cybersecurity controls

Blue Mantis analyzes the 108 controls that comprise the five crucial functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and documents the overall percentage that meet (Pass), don't meet (Fail), and partially meet (Part) those requirements. We then show the results by NIST category (Identify, Protect, Detect, Respond, and Recover) to provide your security risk mitigation roadmap.

Benefits

- Assess risks based on NIST, ISO 27001, and other top security frameworks
- Receive information security plans, incident response playbooks and detailed reporting
- Deploy actionable risk management programs based on business needs

Example results of our Cybersecurity Risk Assessment

