OUR EXPERTISE

As a leading cybersecurity organization and a certified Qualified Security Assessor (QSA) company, GoSecure possesses the expertise and capabilities required to provide an extensive array of services essential for assisting any organizations in achieving and sustaining PCI DSS compliance.

Qualified Security Assessors (QSAs) are independent security organizations that are certified by the PCI SSC to conduct assessments and audits of companies' compliance with the PCI DSS. QSAs perform on-site assessments, review documentation, and provide recommendations for achieving and maintaining compliance.

Approved Scanning Vendors (ASVs) are organizations authorized by the PCI SSC to perform vulnerability scans on external networks and systems. They help identify security vulnerabilities that could be exploited by attackers. ASVs provide reports and recommendations to help organizations address any vulnerabilities discovered during the scanning process.

PCI Security Standards Council (PCI SSC) is the governing body that manages the PCI DSS and related standards. While the PCI SSC itself does not directly provide PCI DSS services, it sets the standards and certification requirements for QSAs and ASVs.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

2023

[Secure Transactions, Assured Compliance]

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. It helps organizations to protect payment card data and meet industry standards.

GoSecure's PCI DSS advisory and compliance offering includes:

- **Scoping/Scope reduction:** Our team of QSAs specializes in delivering cost-effective guidance for achieving PCI DSS compliance, effectively reducing the clients' exposure to card data handling and overall compliance footprint.

- **Gap Analysis:** Once the scope has been defined, GoSecure specialists will engage with the client to assess cardholder data processing activities and practices, comparing them to the Standard to identify any compliance gaps. With the insights from the gap analysis, we will collaboratively develop a compliance strategy.

- **Implementation & Remediation:** Depending on the level of compliance and specific needs, this could be a variety of services, including documentation assistance, security awareness and training or ad hoc advice.

- **Audits or Supported Self Assessments:** Including full audits leading to the issuance of a Report of Compliance (ROC), as well as QSA-led assistance for self-assessment questionnaires (SAQs) against any valid version of the Standard.

- **PCI DSS Consulting:** Through a bank of hours for professional services with an annual expiration, GoSecure clients gain year-round access to our team of QSA advisors, ensuring they can reach out for guidance and support regarding their PCI DSS compliance at any time.

The direction of the mandate will be shaped by your unique objectives and needs. Accordingly, we will execute one or more of the activities detailed in the preceding section, aligned with the project's defined scope.

Note: QSAs are the only third-party entities who can officially co-sign your PCI DSS Attestation of Compliance (AoC) and ROC. We service Canada, Latin America and the Caribbean regions.

[CONTACT US: +1-855-893-5428]

www.gosecure.ai

GOSECURE'S PCI DSS WORKPLAN

- Scoping/Scope Reduction

This phase involves the critical task of defining the boundaries of the cardholder data environment (CDE). The scoping phase holds paramount significance in GoSecure's process, as it sets the foundation for all subsequent phases, shaping the actions and strategies that will ultimately pave the path to compliance achievement.

- Interviews and Observations

Encompasses the assessment of current security practises (including policies, procedures and technical controls) within the defined scope of PCI DSS compliance to identify the areas and systems that do not align with the PCI DSS requirements.

- Implementation & Remediation

Encompasses the guidance for all identified issues in order to meet PCI DSS requirements.

- Reporting

Encompasses the process of compliance reporting. Depending on the organization, this may take the form of a self-assessment questionnaire that GoSecure completes on the client's behalf, with or without the express validation of a Qualified Security Assessor (QSA), or the completion of a ROC and the associated AOC and INFI. GoSecure completes an additional End-of-Project Report for each PCI DSS project.

GENERAL PROCESS FOR MOST PCI DSS MANDATES

SCOPING

- Defining the boundaries of the card holder data environment (CDE).
- Identification and understanding of current payment processes.

INTERVIEWS & OBSERVATIONS

- Identification of the areas that do not align with the PCI DSS requirements.

IMPLEMENTATION GUIDANCE

- Implementation of the compliance strategy.

REPORTING

- Either a full audit or a supported self assessment.

[CONTACT US: +1-855-893-5428]

GoSecure is a recognized cybersecurity leader and innovator, pioneering the integration of endpoint, network, and email threat detection into a single Managed Extended Detection and Response (MXDR) service. The GoSecure Titan® platform delivers predictive multi-vector detection, prevention, and response to counter modern cyber threats. GoSecure Titan® MXDR delivers rapid response and active mitigation services that directly touch the customers' network and endpoints. For over 20 years, GoSecure has been helping customers better understand their security gaps and improve their organizational risk and security maturity through MXDR and Professional Services solutions delivered by one of the most trusted and skilled teams in the industry. To learn more, please visit:

www.gosecure.ai

Your ally to consolidate, evolve & thrive

GOSECURE