OPSEC | SAQ Risk Assessment

For When You Need More Insight

The SAQ focuses on 25 key areas of cybersecurity posture based on established standards such as the NIST Cybersecurity Framework and the Center for Internet Security's Critical Security Controls. Response options are standardized to ensure consistency among vendors while remaining flexible to accomodate variances. For improved accuracy, up to three participants from an organization can be assigned to validate the responses.

OPSEC | SAQ Capabilities

99 Evaluation Questions
Questions assess security objectives in 25 key areas of cybersecurity according to NIST and CIS frameworks.

Additional Support Requirements
Optionally request risk management info (PoAMs, compensating controls, or risk acceptance) for each objective. Collect evidence to verify SAQ responses, which will be reviewed manually to ensure compliance.

Scoring Dashboard
Utilize the dashboard to respond, review, and remediate. Responses are dynamically scored and can be reviewed post-completion. As remediations are completed, an additional score is provided to reflect progress.

When to Choose OPSEC | SAQ

SELECT vendors and conduct evaluations

VALIDATE vendor compliance

ONGOING vendor management

Implement corrective action

EXPAND OR CONTRACT vendor relationships

TERMINATE vendor relationships

How Is OPSEC | SAQ Different?

Replace Spreadsheets Send, receive, and manage SAQs digitally.

Standardize Questionnaire Scoring Use consistent questionnaire and response methods to score and rate.

Mutually Track Improvements Provide dashboards for both parties to track improvements post-questionnaire.

Share Data Vendors can easily share data with other organizations upon receiving more requests.

myCYPR™

6315 Hillside Court, Ste J
Columbia, MD 21046
United States

410-292-7601
info@anchortechnologies.com
www.mycypr.com