

HIPAA Security Risk Analysis

Objective

Assess the organization against the HIPAA Security Rule to identify gaps in security control coverage and make recommendations for improvement.

Outcomes

1

Documentation of current state, gaps, and risks associated with established controls, mapped to selected frameworks.

2

Analysis of risks and threats unique to the organization.

3

Recommendations to close gaps.

4

Risk Management Plan for organization to track remediation process.

High Level Approach

SCOPE IDENTIFICATION

SRA will provide a request for information to obtain compliance and security documentation, as well as to assist in scheduling interviews with stakeholders.

HIPAA / HITECH GAP ASSESSMENT

SRA will conduct a series of interviews to help assess the organization's alignment with the intent of the HIPAA security rule.

RISK ANALYSIS AND REPORTING

SRA will document the results of the risk analysis and conduct a workshop to discuss recommendations.

Differentiators

Healthcare Experience

SRA has significant experience assessing clients in the healthcare sector, enabling us to benchmark results from similar clients. Our methodology incorporates the intent of the HIPAA Security Rule, recent HICP guidance, our experience working with HHS, and lessons learned from our past projects with similar clients.

Thought Leadership

Security Risk Advisors contributes to cybersecurity thought leadership conferences, including RSA, Gartner, ISC(2), FS-ISAC, NH-ISAC and other knowledge-building organizations. In 2017 we released a cutting-edge freeware reporting and workflow tool for measuring CyberSOC detection rates and improvement.

Technical & Compliance Roots

Our strategy team leads have deep experience understanding both technical and compliance-oriented complexities of large organizations. We focus on working with top market clients, but we also maintain broad perspective by working with innovating technology start-ups and mission-oriented non-profits.