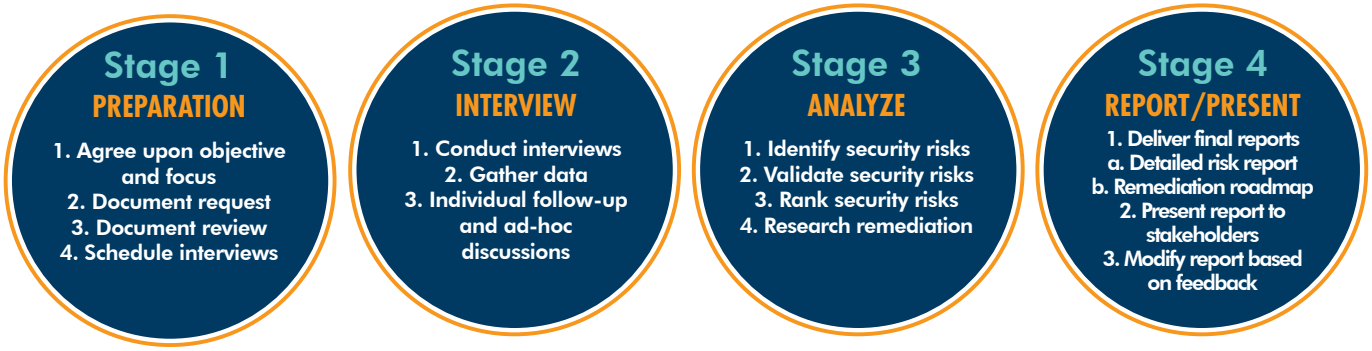
SECURITY PROGRAM ASSESSMENT

Using industry best practices, along with our own proprietary tools and methodologies, SageNet's cyber-risk assessments identify gaps and vulnerabilities in security programs. We deliver an actionable roadmap to best practices and compliance; strengthening overall security, reducing risk and providing better protection against both internal and external threats. Our Risk Assessment services include:

- ISO 27002 or NIST framework to evaluate information security controls
- Roadmap to compliance assessment (Not auditors, but agents for change)
- Focused cyber risk assessments on specific technologies (Firewall review, IPS config, etc)
- Cyber Incident Response planning
- Third party or cloud risk assessments
- Application security assessments, code review, and testing

PROCESS

In an effort to provide the most comprehensive roadmap, SageNet utilizes a multi-phased approach when assessing an organization's security program. Our goal is to help our clients move toward a more secure cyber environment amidst the ever-changing threat landscape.



Your organization's enterprise has never been more valuable, and vulnerable. SageNet will assess your security program to give you a roadmap that will minimize your risk in a strategic way. Our team consists of experienced professionals with certifications including CISSP, HCISPP, CISA, CISM, CEH, CHFI as well as many vendor-specific certifications. We are ready, willing and able as we help you to apply your resources in the most effective way.

sageSECURE™

ASSESSMENT OVERVIEW

Preparation

Kickoff meeting to review:

- Key personnel
- Framework requirement (ISO, NIST, GDPR)
- Compliance drivers (PCI, FDIC, NCUA, FISMA)
- Environment scope
- Documentation request
- Schedule for interview
- Interview expectations
- Timeline for report delivery

Particular emphasis is given to understanding the strategic objectives of the organization, where the current state may be falling short of those objectives, and where broader corporate organizational or environmental issues are influencing the effectiveness of the current processes.

Interview

During this phase of the assessment, SageNet will meet with selected members of the client's staff in roles related to the information security program.

- IT Security
- IT Infrastructure
- Software Development
- Human Resources
- Legal
- Physical Security

Analysis

The collected data and the various observations are collated and analyzed to identify the overall state of the information security program. Follow-up meetings with client staff members may occur for any gaps in information or understanding.

Report

During this phase, SageNet reviews the overall results of the assessment process in a logical manner.

- Observations and recommendations are compared to the initial objectives identified early in the assessment process such that the benefits of the key actionable recommendations are clear.
- Specific areas where the current processes or approach can be improved are identified as a result of the gap analysis approach.
- Positive observations are included to ensure good elements of the program are highlighted.

Present

At the end of the engagement, SageNet provides an opportunity to review the report with the client's management team and assessment stakeholders.