SHARED ASSESSMENTS

TRUST

Why Should I Accept The **SIG**?

*More than **500 organizations and partners** license the Standardized Information Gathering (SIG) Questionnaire for security due diligence with **tens of thousands of clients and vendors** who accept the SIG as the industry-standard.*

The SIG is vetted by industry leaders to satisfy diligence requirements for any level of risk a business needs to assess. Designed for assessing service providers managing sensitive or regulated information, the SIG is also meant for systems and services whose availability is highly critical to business operations.

Based on relevant industry standards, frameworks, and regulations, the SIG provides a deep level of understanding about how a service provider secures information and services.

100K+

SIGs Exchanged Annually

70%

Acceptance Rate For Assessment Requests

OUTSOURCER EFFICIENCIES

An Outsourcer can create an output report based on conflict between their **Ideal Response Key** and the Vendor's response.

VETTED BY ALL FACETS OF TPRM

Service Providers, Outsourcers, Assessment Firms, and Vendor Risk Management Platforms all contribute to create the depth and breadth of the **SIG Content Library**.

SIG+SCA

The Shared Assessments **Standardized Control Assessment (SCA)** Procedures verify risk control through attestation of SIG responses.

Scalable Savings

Accepting Service Provider SIG responses promotes efficiency and timeliness:

Without SIG
50 assessments
x 8 hours each
x $50/hour
$20,000

With SIG
50 assessments
x 2 hours each
x $50/hour
$5,000

**For illustration only, results vary*

Learn More: www.sharedassessments.org/sig

21 RISK DOMAINS

Access Control
Application Security
Artificial Intelligence (AI)
Asset and Information Management
Cloud Hosting Services
Compliance Management
Cybersecurity Incident Management
Endpoint Security
Enterprise Risk Management
Environmental, Social, Governance (ESG)
Human Resources Security
Information Assurance
IT Operations Management
Network Security
Nth Party Management
Operational Resilience
Physical and Environmental
Privacy Management
Server Security
Suppy Chain Risk Management (SCRM)
Threat Management

MAPPING REFERENCES

Technology Standards/Frameworks
Shared Assessments SCA 2024
ISO 27001:2022
ISO 27002:2022
ISO/IEC 27701 PIMS A 2019
NIST Artificial Intelligence 100-1 2023
NIST SP-800-161r1 2022
NIST SP-800-53r5 Sep 2020
NIST Cybersecurity Framework Apr 2018
NIST Privacy Framework Jan 2020
Cybersecurity Maturity Model Certification (CMMC) 2.01 2021
CIS Critical Security Controls v8 2021

Regulations, Statutes and Laws
EBA Guidelines on Outsourcing Arrangements Feb 2019
EU GDPR 2016/679
Interagency Guidance on Third-Party Relationships
FedRamp May 2021
FFIEC CAT Tool May 2017
FFIEC IT Exam Handbook: AIO Jun 2021
FFIEC IT Exam Handbook: Business Continuity Nov 2019
FFIEC IT Exam Handbook: Mgmt Nov 2015
FFIEC IT Exam Handbook: Outsourcing Jun 2004
HIPAA Administrative Simplification Mar 2013
NYDFS 23 NYCRR 500 Mar 2017

Industry Sector Guidance
CSA CAIQ 3.1 Apr 2020
CSA Cloud Controls Matrix v4
ISA 62443-4-1- and 2 2018
NERC
PCI DSS 4.0 March 2022

ABOUT SHARED ASSESSMENTS: DRIVING TRUST IN THIRD PARTY RELATIONSHIPS

Shared Assessments was founded by large banks, service providers and major accounting firms to create standards and efficiencies in third-party risk assessments.

Today, our members and risk professionals span all major industry verticals, including energy, government, healthcare, information technology, manufacturing, and retail.

Third-party risk management is a relationship business. Our greater community is essential to what we do. Our focus continues to be working together to create a more secure and resilient world.

BOOK A DEMO
sharedassessments.com