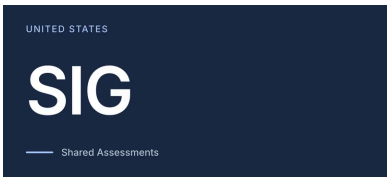
SmartSuite

Framework / Supply Chain Security / Other

Standardized Information Gathering (SIG) Questionnaire, Shared Assessments

The Shared Assessments SIG is the licensed, annually updated third-party risk questionnaire covering 21 risk domains, delivered as an Excel workbook or the SIG EV web platform.



What it is

The Standardized Information Gathering (SIG) questionnaire is the licensed third-party risk questionnaire published by Shared Assessments LLC, a membership organization that has been part of OneTrust since 2021, which outsourcers send to their service providers to collect answers about security, privacy, resilience and compliance controls across 21 risk domains. It is updated every year, sold as an annual corporate license (listed at $7,000 for one year) and included with all levels of Shared Assessments membership, and since 2026 it is delivered both as the SIG Excel workbook and as SIG Evolution (SIG EV), a web-based platform for creating, sharing, scoring and validating assessments.

At a glance

PUBLISHER
Shared Assessments LLC (a membership organization, part of OneTrust since 2021)

TYPE
Standard

VERSION
Annual release; 21 risk domains; delivered as SIG Excel (with SIG Manager) and SIG EV (web platform); mapped to SCA 2026

EFFECTIVE
Each annual release applies on publication; the current release is listed on the publisher's SIG page

DOMAIN
Supply Chain Security

FAMILY
Other

REGION
United States (used globally)

ADOPTION MODEL
Industry Requirement

IMPLEMENTATION COMPLEXITY
Medium

Source: sharedassessments.org/sig-ev/

Why it matters

- **One questionnaire the market accepts** A vendor's completed SIG serves many customers; an outsourcer's reviewers see a familiar structure instead of a bespoke spreadsheet from each business unit.
- **21 risk domains** Access control, application management, artificial intelligence, asset and information management, cloud services, compliance, incident management, endpoint security, enterprise risk, ESG, HR security, information assurance, IT operations, network security, Nth-party management, operational resilience, physical security, privacy, server security, supply chain risk and threat management.
- **Mapped to the rules you answer to** Each question carries mappings to the standards and regulations the publisher lists, so answers can be read as evidence against ISO/IEC 27001, NIST SP 800-53, PCI DSS, HIPAA, the GDPR, DORA, NIS 2 or NYDFS 23 NYCRR 500.
- **Annual, versioned, traceable** A new SIG each year with a SIG Manager Enhancement Document describing the changes and a Version Delta tracing every question back to 2008.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Shared Assessments SIG

Vendor Inventory and Scoping

Hold every third party with its criticality, data access and services, and record which SIG scope and release year it received.

SIG Response Intake

Capture the completed SIG workbook or SIG EV export per vendor with the 21 risk domains as structured sections and the supporting files attached to the questions they answer.

Domain Scoring and Findings

Score answers by risk domain, log gaps as findings with owner and due date, and track vendor remediation to closure.

SCA Verification

Plan and record Standardized Control Assessment procedures for vendors whose self-attested answers need testing, with results linked back to the SIG questions.

Mapping to Obligations

Link SIG answers to the controls and regulatory requirements in Compliance Management (ISO/IEC 27001, NIST, DORA, NYDFS 500, PCI DSS) so vendor evidence serves your own audits.

Annual Refresh and Reporting

Schedule the yearly re-assessment on the new SIG release, carry prior answers forward using the Version Delta, and report vendor risk posture and open findings to management.

Common framework mappings

COBIT 2019 | GDPR | HIPAA | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

Shared Assessments SIG 2024 Questionnaire

Official document providing standardized information gathering questions for third-party risk assessments.

sharedassessments.org/sig

Shared Assessments Best Practices

Describes best practices for implementing the SIG framework effectively.

sharedassessments.org/resources

SIG Implementation Guidance

Provides practical guidance for organizations using the SIG in third-party risk management.

sharedassessments.org/sig-implementation

Shared Assessments Framework Overview

Outlines the structure and components of the Shared Assessments framework.

sharedassessments.org/framework-overview

Frequently asked questions

What is the Shared Assessments SIG questionnaire?

The Standardized Information Gathering (SIG) questionnaire is a licensed set of third-party risk questions published by Shared Assessments LLC. Outsourcers send it to service providers to collect answers about their controls across 21 risk domains, and the answers are mapped to the regulations and standards the publisher lists, from ISO/IEC 27001 and NIST SP 800-53 to the GDPR, DORA, HIPAA and PCI DSS. It is available as the SIG Excel workbook with the SIG Manager tool and as SIG EV, a web platform.

What are the 21 SIG risk domains?

Access Control; Application Management; Artificial Intelligence (AI); Asset and Information Management; Cloud 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 Security; Privacy Management; Server Security; Supply Chain Risk Management (SCRM); and Threat Management, as listed on the publisher's SIG page.

How is the SIG licensed and what does it cost?

The SIG is a paid product. The publisher lists a corporate license at $7,000 for one year, offers multi-year pricing on request, and includes the SIG with all levels of Shared Assessments membership. The license includes the SIG itself with the SIG Manager, the SIG User Guide, the SIG Manager Enhancement Document describing the current release's changes and the SIG Version Delta workbook.

Is the SIG a certification or a legal requirement?

No. The SIG is a questionnaire and content library, not a control standard, and completing it does not certify a vendor. No law mandates it, but outsourcers commonly make a completed SIG a contractual condition of doing business, and regulators that require third-party due diligence (for example under DORA or NYDFS 23 NYCRR 500) accept it as the collection method, which is why it functions as an industry requirement.

How does the SIG relate to the Standardized Control Assessment (SCA)?

The SIG collects a vendor's self-attested answers; the SCA is Shared Assessments' set of procedures for testing those controls on site or virtually. The current SIG is mapped to the SCA 2026 procedures, so an outsourcer can move from a questionnaire answer to a verification step without re-mapping the control. Shared Assessments also publishes the VRMMM maturity model and the TPSIRR review alongside the SIG.

License included / downloadable: No The SIG is licensed by Shared Assessments LLC: a corporate license listed at $7,000 for one year, multi-year pricing on request, and inclusion in all levels of Shared Assessments membership. The platform does not include the question set; licensees load their own copy.

Full framework page and mappings: smartsuite.com/frameworks/shared-assessments-sig-standardized-information-gathering

© 2026 SmartSuite Inc. All rights reserved.