SCHNEIDER DOWNS
Big Thinking. Personal Focus.

OUR THOUGHTS ON

Third Party Risk Management Insights

Shared Assessment SIG Questionnaire – What's New for 2023?

Do you ever feel the burden of endless third-party questionnaires?

Do they seem to be slightly different, yet similar at the same time? Do they seem to relate to various other frameworks that you follow and document, but they are not exactly the same?

If you feel any of these frustrations, some of the changes made to the Shared Assessments 2023 Standardized Information Gathering (SIG) Questionnaire may provide you a little sigh of relief!

For those that are not familiar, the SIG Questionnaire is a widely accepted tool that is used by many organizations as a part for their third-party risk management process, with the goal of a standardized questionnaire that can be used and relied upon in the industry.

As 2022 is quickly rolling to a close, we are seeing the beginning of releases for new templates and guidance for 2023. One of those new releases is the 2023 Shared Assessment Third-Party Risk Management Product Suite, which includes the updated SIG Questionnaire.

The various changes and additions to the SIG Questionnaire for 2023 will ensure that organizations have adequate coverage of all key and emerging risks as well as streamline the process and provide enhanced mapping to additional existing frameworks to avoid duplication of efforts, where possible.

The changes to the 2023 SIG fall into three buckets:

Clarity/Organization/Functionality As the SIG Questionnaire is a very large, comprehensive tool, it requires frequent updates to ensure that it remains relevant, clear, concise, and user friendly. Shared Assessments updated 1,600 control points, retired legacy questions, assigned “control category” and “control attribute” to all questions, improved visibility to content across domains, expanded content based on mapping reference documents, reorganized questions in each domain by topic and sequence for easier evaluation, as well as made functionality enhancements to the template.

Risk Domain Updates As emerging topics and trends fluctuate, Shared Assessments re-evaluates the Risk Domains within the SIG Questionnaire to ensure adequate coverage, while maintaining efficiency and alignment. This year, there were four updates to the Risk Domains. First, for greater visibility, a Risk Domain was added to migrate existing Environment, Social, and Governance (ESG) content form the Compliance and Operations Risk Domains into its own Risk Domain. Second, after the ESG questions were migrated to their own Risk Domain, the Compliance Risk Domain was renamed to Compliance Management. hird, the Security Policy and Organization Security Risk Domains were merged together to create Information Assurance. Lastly, the Fourth Party questions were moved into their own Risk Domain for greater visibility as this continues to be an area of focus for organizations and regulators.

New Key Mappings The DOE announced that it is accepting public comment on the announced guidance for 30 days (now through March 30). One comment from regulations.gov brought to light a perspective of these new changes from an employee at small college with a religious mission that involves maintaining very low tuition costs for students, many of whom come from lower socioeconomic backgrounds. The comment highlights two negative possibilities from the DOE update.

First, the institution's partners could become TPSs, creating associated increased costs that the college would need to fund, likely ultimately increasing student costs.

Second, the institution partners could decline to become TPSs, in which case schools would have to cease operations, disrupting academic operations, especially in smaller, less-resourced institutions.

Smaller Businesses In efforts to allow the SIG Questionnaire to be widely used and cross-referenced to existing standards/guidelines, Shared Assessments completed four new key mappings and two special initiatives. The SIG Questionnaire was newly mapped to the following four standards: Federal Financial Institutions Examination Council (FFIEC) Outsourcing Technology Services guidance, the Federal Financial Institutions Examination Council (FFIEC) Architecture, Infrastructure, and Operations (AIO) guidance, the Federal Risk and Authorization Management Program (FedRAMP), and the North American Electric Reliability Corporation (NERC) Reliability Standards. Additionally, one of the special initiatives for the year was around ESG and expanding the depth of coverage of this topic. Finally, Shared Assessments has partnered with Secure Controls Framework (SCF) and will now be able to map directly to SCF's comprehensive controls catalog and mappings using questions in the SIG Questionnaire. This collaboration expands the SIG Questionnaire library related to frameworks, laws, and regulations.

In addition to the SIG Questionnaire, Shared Assessments also offers the Standardized Control Assessment (SCA) Procedure and a Vendor Risk Management Maturity Model (VRMMM) that were also updated for 2023 as well.

Although these tools are less widely used, they are great resources to help your organization depending on the stage that your third-party risk management program is currently in.

How Can Schneider Downs Help?

Schneider Downs is a registered assessment firm with the Shared Assessments Group, the clear leader in third-party risk management guidance. Our personnel are experienced in all facets of vendor risk management, and have the credentials necessary (CTPRP, CISA, CISSP, etc.) to achieve meaningful results to help your organization effectively achieve new vendor risk management heights.

For more information, please visit www.schneiderdowns.com/tprm or contact us at contactsd@schneiderdowns.com