Top 11 IT Vendor Assessment Questionnaires of 2022

1. California Consumer Privacy Act (CCPA) Questionnaire

The California Consumer Privacy Act (CCPA) or AB 375 is a new law that became effective on January 1, 2020, designed to enhance consumer privacy rights and protection for residents in the state of California by imposing rules on how businesses handle their personal information.

The CCPA is the most extensive consumer privacy legislation to pass in the United States and is akin to the European Union's General Data Protection Regulation (GDPR) and other data privacy laws and privacy regulations.

Like GDPR, CCPA is an extraterritorial law that applies to all organizations, regardless of whether they operate in California.

2. Center for Internet Security — CIS Critical Security Controls (CIS First 5 / CIS Top 20)

The CIS Controls for Effective Cyber Defense are a prioritized set of actions that form a defense-in-depth set of specific and actionable best practices to mitigate the most common cyber attacks.

They were created and maintained by the Center for Internet Security (CIS), a forward-thinking nonprofit that harnesses the power of a global IT community to safeguard public and private organizations against cyber threats.

The CIS controls embody the first steps to securing the confidentiality, integrity, and availability of an organization, and can be considered a short-list of high-priority, highly effective defensive actions for any vendor seeking to improve their cyber defense.

The first five CIS Controls are often referred to as providing cyber hygiene and studies have shown that their implementation provides an effective defense against the most common cyber attacks (~85% of attacks).

Additionally, the CIS Controls map to many major compliance frameworks such as the NIST Cybersecurity Framework, NIST 800-53, ISO 27000 series, and regulations such as PCI DSS, HIPAA, NERC CIP, and FISMA.

3. Cloud Security Alliance — Consensus Assessments Initiative Questionnaire (CAIQ)

The Consensus Assessments Initiative Questionnaire (CAIQ) is a security assessment provided by the Cloud Security Alliance (CSA), a leading organization dedicated to defining and raising awareness of secure cloud computing best practices. The CAIQ helps cloud consumers and auditors assess the information security capabilities of data center and cloud providers.

The CAIQ was created to address one of the leading concerns organizations have when moving to the cloud, namely the lack of transparency into what technologies and tactics cloud providers implement, relative to data protection and risk management.

It provides commonly accepted industry standards to document security controls in IaaS, PaaS, and SaaS offerings.

The CAIQ does this through a series of "Yes/No" questions designed to ascertain compliance with the CSA Cloud Controls Matrix (CCM) which is composed of 133 control objectives structured across 16 domains that cover all key aspects of cloud technology.

4. General Data Protection Regulation (GDPR) Questionnaire

The General Data Protection Regulation (GDPR) is an extraterritorial European law that applies to the processing, storage, and exposure of personally identifiable information (PII) of European citizens.

Compliance with GDPR also means compliance with other privacy laws such as CCPA, LGPD, the SHIELD Act, FIPA, and PIPEDA.

While many organizations know they must process data in accordance with GDPR, many forget that GDPR is focused solely on data, which means that any data that passes through or is stored with a vendor must also comply with GDPR.

Additionally, GDPR requires that organizations report data breaches within 72 hours to the appointed Data Protection Authority (DPA), who will handle the legal ramifications of the data exposure, which can result in fines up to €20 million or 4% of annual global revenue, whichever is higher.

To get visibility on your vendor's compliance with GDPR, you'll need to develop a robust GDPR questionnaire or use the one available on the UpGuard platform.

5. Higher Education Community Vendor Assessment Tool — (HECVAT / HECVAT Lite)

The Higher Education Community Vendor Assessment Tool (HECVAT) is a security assessment template that generalizes higher education information security and data protection questions, as well as issues regarding cloud services for consistency and ease of use.

HECVAT has various versions that are free to use and provide a consistent, streamlined third-party risk assessment framework:

- **HECVAT:** 265 questions including qualifying questions for HIPAA and PCI-DSS opt-in
- **HECVAT Lite:** A lightweight questionnaire used to expedite the process
- **On-premise:** A unique questionnaire used to evaluate on-premise applications and software

HECVAT was created by the Higher Education Information Security Council (HEISC) Shared Assessment Working Group, EDUCAUSE, Internet2, and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).

6. ISO 27001 Questionnaire

ISO/IEC 27001 is one of the most well-known and well-used information security standards and is part of the ISO/IEC 27000 family of standards. It is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO 27001 takes a systematic approach to vendor risk management by running standard risk assessment and compliance checks, then providing suggestions and action plans to treat and prevent issues in the future.

One of the biggest benefits of using the ISO 27001 questionnaire is that it proactively identifies how vendors are utilizing resources and tools incorrectly, which is often what results in compliance gaps and security threats in the first place.

7. Modern Slavery Questionnaire

The Modern Slavery Questionnaire is aligned with Australia's Modern Slavery Bill 2018 and the UK's Modern Slavery Act 2015.

It is designed to help support you in identifying any modern slavery risks, enable collaborative efforts between third-parties and organizations to address the risks, improve transparency, and identify areas for further due diligence.

8. National Institute of Standards and Technology — NIST SP 800–171

NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171) provides federal agencies with a set of guidelines designed to ensure that Controlled Unclassified Information (CUI) remains confidential, available, and unchanged in nonfederal systems and organizations.

NIST SP 800-171 contains 14 specific security objectives, each with a variety of unique controls.

Any federal agency that engages with third-parties and any nonfederal systems or organizations that are used by federal agencies must comply with NIST 800-171.

By complying with NIST SP 800-171, you will also meet the majority of the criteria for NIST SP 800-53 and compliance with NIST SP 800-53 is a major part of FISMA and FedRAMP compliance.

While NIST SP 800-171 mainly focuses on companies that work under a government contract, it represents a concerted effort to improve cybersecurity at a national level and is a detailed framework that can be used by any organization looking to improve its cybersecurity posture.

9. Shared Assessments Group — Standardized Information Gathering Questionnaire (SIG / SIG-Lite)

The Standardized Information Gathering (SIG) questionnaire is used to perform an initial assessment of vendors, gathering information to determine how security risks are managed across 18 different risk domains.

SIG was developed by Shared Assessments and is a holistic tool for risk management assessments of cybersecurity, IT, privacy, data security, and business resiliency.

There are three types of SIG questionnaire:

1. **SIG questionnaire:** The SIG assessment evaluates vendors based on 18 individual risk controls, which together determine how security risks are managed across the vendor's environment.
2. **SIG LITE:** The SIG questionnaire is extensive, targeting multiple risk areas across multiple disciplines. For vendors who have less inherent risk, who don't require the entire SIG assessment, SIG LITE can be valuable. It takes the high-level concepts and questions from the larger SIG assessments, distilling them down to a few questions.
3. **SIG CORE:** SIG CORE is a library of questions that security teams can pick and choose from, including extensive questions about GDPR and other specific compliance regulations.

10. Vendor Security Alliance — VSA Questionnaire (VSA)

The Vendor Security Alliance (VSA) questionnaire was created by a coalition of companies committed to improving Internet security.

The VSA issues two free questionnaires which are updated annually:

- **VSA-Full:** This is the classic VSA questionnaire that focuses deeply on vendor security and is used by thousands of companies globally.
- **VSA-Core:** This questionnaire is comprised of the most critical vendor assessment in addition to privacy. The privacy section covers both US data breach notification requirements, the California Consumer Privacy Act (CCPA), and the General Data Protection Regulation (GDPR).

Unlike other questionnaires, the VSA assessment process was created with the vendor in mind. Its focus is to eliminate irrelevant questions, reducing the time it takes for InfoSec and security teams to complete the questionnaire.

11. Payment Card Industry Data Security Standards (PCI DSS) Questionnaire

The Payment Card Industry Data Security Standards (PCI DSS) is an information security and data security standard for organizations that handle branded credit cards from the major card schemes.

In 2006, five major credit card companies–Visa, MasterCard, Discover, American Express, and JCB, came together and established the Payment Card Industry Security Standards Council (PCI Security Standards Council or PCI SSC) to administer and manage security standards for companies that handle credit card data.

Any organization who accepts or processes payment cards must be PCI compliant which involves three main things:

1. Ensuring that sensitive card details are collected and transmitted securely
2. Storing data securely by meeting the 12 security domain requirements of the PCI standard, such as encryption, continuous monitoring, and security testing of access control to card data
3. Annual validation that required security controls are in place, which can include forms, security questionnaires, external vulnerability scanning, and third-party audits.

Which Questionnaire is Right For Your Third-Party Risk Management (TPRM) Program?

Determining the right assessment tool for your organization's vendor risk management (VRM) program isn't something to take lightly. However, the number and quality of security questionnaires available for use are continually increasing.

The majority are regularly updated and improved (typically on an annual basis) by groups of experts in cybersecurity, information security, compliance, and risk, and are increasingly adopted by the world's leading companies.

If you're not sure which questionnaire or framework is right for you, let our team help you decide or use our library of pre-built questionnaires that can simplify the process and save your team significant time and resources.

Why You Should Consider Using Security Ratings Alongside Vendor Questionnaires

Security ratings provide risk management and security teams with the ability to continuously monitor the security posture of their vendors.

The benefit of security ratings alongside security questionnaires is they are automatically generated, updated frequently, and they provide a common language for technical and non-technical stakeholders.

The key thing to understand is that security ratings fill the large gap left from traditional risk assessment techniques like security questionnaires. Sending questionnaires to every third-party requires a lot of commitment, time, and frankly isn't always accurate.

Security ratings can complement and provide assurance of the results reported in security questionnaires because they are externally verifiable, always up-to-date, and provided by an independent organization.

According to Gartner, *cybersecurity ratings will become as important as credit ratings when assessing the risk of existing and new business relationships…these services will become a precondition for business relationships and part of the standard of due care for providers and procurers of services.*