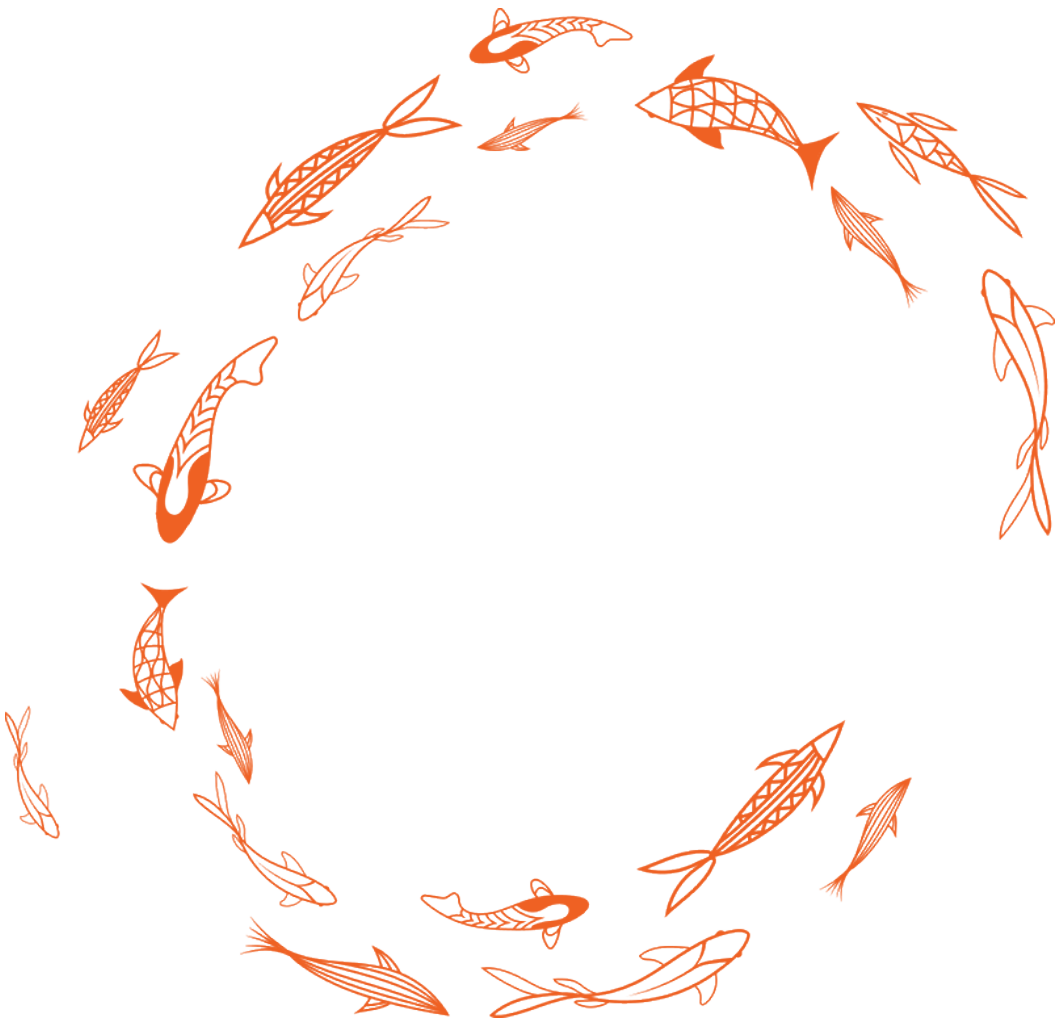
blue umbrella
making business better

Guide | Understanding Third-Party Risk Management Questionnaires

Third-Party Risk Management Questionnaires: What You Should Know



Read This Before Developing a Third-Party Risk Management Questionnaire

Risk assessment questionnaires represent a critical part of the overall third-party risk management process. This important (and usually first) step helps determine whether a third party is low, medium or high risk and what actions follow as a result of the information that is uncovered or disclosed. There are many different types of risk a third party may present to your company, including IT security, data privacy, anti-bribery and corruption and any number of other regulatory or industry-specific compliance areas. A survey we conducted of compliance professionals at mid-size companies indicated **IT security and data privacy** were the most pressing third-party risk areas.

Our recent survey indicated **80% of respondents** felt IT security was a top compliance area of concern.

Although IT security and data privacy do top the list of third-party risk areas, it's most often the general counsel or head of legal who is tasked with implementing the program to manage this risk. Or, in many cases, it's up to the general counsel to work with IT and procurement to make it happen. Lack of expertise on IT security and data privacy can be a concern for these great legal minds, so often the first place they turn to get an idea of where to start is Google. On top of the lack of confidence in the subject matter, getting internal consensus around which questions to ask in a risk management questionnaire can be difficult. Inter-departmental teams may struggle to determine the length and depth needed to adequately assess the risk with a third party and there may be different objectives or tolerance to risk at play.

The reality is the regulatory environment is always changing. Look at how the introduction of the California Consumer Privacy Act (CCPA) changed how companies handle and store their customer's data. Developing a risk assessment questionnaire internally can take **extensive time and resources**. Alternatively, working with external experts to rubber stamp their own version of a risk assessment questionnaire can take a substantial chunk of your budget. What's a general counsel or compliance professional to do in this situation? We suggest you read on.

Finding a Questionnaire Online Can Be Risky

The regulatory environment is a living, breathing thing, with new laws coming into effect (CCPA, for example) and increased scrutiny from regulators forcing companies to simultaneously focus their attention in multiple directions. Sure, it's easy enough to find samples of third-party

Check out our guide on this topic:
Five Third-Party Compliance Lessons to Learn from Fortune 500 Companies.

risk management questionnaires online, but it's extremely difficult to determine their quality or if important questions are missing. Not to mention identifying when these sample questionnaires were created or how recently they have been updated. Using a questionnaire template you find online can put you and your organization at risk if the content is weak or if a critical question or series of questions have been overlooked.

So, how does one determine the quality of a third-party risk assessment questionnaire? A good third-party risk assessment questionnaire is strongly aligned with best practices. It is often the companies with the most risk (Fortune 500 companies, for example) who dedicate the time, expert brainpower and resources to establish the most thorough and relevant risk assessment questionnaires. At the end of the day, how these world-leading organizations assess third-party risk is a good yardstick for the rest of us. Learning from their approach and how they have established best practices in key third-party risk areas is important.

If you don't have the internal expertise on a key third-party risk area or the budget to hire external counsel, then using a **gold standard risk assessment questionnaire** will give you confidence that nothing is getting overlooked and that you're aligned with best practices. Working with a trusted provider specializing in third-party risk will allow you to rest easy knowing your bases are covered and that your questionnaire is grounded in best practices developed by the world's most sophisticated programs.

Key Subject Areas for Risk Assessment Questionnaires

As we described above, most general counsels or individuals overseeing the development or distribution of third-party risk management questionnaires are not subject matter experts on every risk area they need to manage. (Hence the natural inclination to turn to Google for answers.) Here we will outline some of the key subject areas for the most common third-party risk assessment questionnaires so you can better identify a good one when you find it.

Anti-Bribery and Corruption

- Ownership and management
- Government connections
- Compliance history
- Compliance program
- Services
- Data protection

Data Privacy

- Roles
- Nature and Purpose
- Policies and Processes
- Privacy by Design
- Use of Third Parties
- Incident Response and Management
- IT Governance
- Access Management
- Data Transfer

IT Security

- Engagement Details
- IT Governance
- Human Resources
- Access Management
- Network Security
- Change Management
- Development and Maintenance
- Mobile Security
- Data Retention and Removal
- Physical Security and Asset Management
- Security Assessment
- Business Continuity Plan
- Incident Response and Management

These categories give you an idea of the critical questions that should be included in your questionnaire to align with best practices. This helps ensure you are considering every possible subject-related risk area with your third-party relationship.

We Have the Best Possible Questionnaire. Now What?

Unfortunately, finding or developing a risk assessment questionnaire is only the start of the process. Even if you develop your own proprietary third-party risk assessment (read our take on that above), you still have to distribute it, collect the responses, assess the risk, track the remediation efforts and more. Based on our research, this process typically involves using **3.6 tools**, including email, survey management software, spreadsheets, file storage and more. It quickly becomes complicated and can be difficult to scale because of the manual processes involved. Furthermore, it is exceedingly difficult to retain proper, centralized records in the event an enforcement agency comes knocking at the door.

Hey, guess what? Technology helps. Having the right system in place to automate the distribution and collection of risk assessment questionnaires, flag the risks and allow for centralization of data is invaluable. Additionally, having a way to help support internal collaboration and accountability around remediation of identified risk is also important. This will save you countless hours and headaches and will help you feel confident you can focus your attention on the most important areas instead of wondering, “Wait, did that vendor even send back the questionnaire?”.

While the quality and content of the third-party risk assessment questionnaire is critical, having a sound technology in place to help you manage the process is equally so.

Care to learn more about how the combination of gold standard risk assessments and powerful, intuitive technology can turn your third-party risk management program around? Watch a product tour of Blue Umbrella GRC, our modular third-party compliance and risk management software built especially for mid-size companies. And reach out to us if you would like to chat more.

Get complete visibility of multiple areas of third-party risk with your vendors, distributors and agents.

Learn More Today

Starting a third-party compliance program to gain critical visibility to risk is easy with Blue Umbrella GRC.

Our suite of third-party risk management modules allows you to distribute gold standard risk management questionnaires to your business partners, track their progress and analyze the results for efficient follow-up. It's a plug & play solution designed to get you up and running within minutes. With no time to lose, why not start now? Watch a video introduction.