

Third-Party Risk Prioritization Checklist

The traditional method of assessing third parties is broken. Many companies send out ineffective questionnaires that do not address risk because they lack the resources to support a proper program and simply need to check a box. The first step to a quality third-party risk program? Focus on establishing a robust method for prioritization and focus your resources on critical third parties.

Understand the third parties that present the most risk by following this prioritization checklist:

- Have an accurate inventory of vendors and filter by security concerns.** Third-party lists become outdated because of changes in POC's and services offered. As simple as it seems, maintaining an accurate inventory is a step often overlooked. Next, organize by security concern (companies that store your data, have access to your environment, or that provide a tool or software) and create an assessment approach by vendor type/priority. Focus your efforts only on those vendors that need to be assessed.
- Tailor the required controls based on the services/products being provided.** Asking about access controls and encryption makes sense for a vendor that is storing your data. In this case, requesting background checks or general information about security policy would provide little to no value. Instead, why not focus on the data encryption standards or change control procedures which could directly impact your data?
- Avoid generic questionnaires at all costs.** Why send a blanket questionnaire to your third parties when you lack a clear understanding of what they do for you? Generic questions will get broad answers and convoluted results. Instead, be more focused and prescriptive in what controls you expect of the third party and how they directly address risks to your organization.
- Treat your TPRM program as a partnership with the third party.** Organizations may need time to adhere to your control requirements, especially when working with small organizations and startups. Working with a third party as part of a corrective action plan (CAP) process could help build the relationship, support the business, and provide better visibility into the controls being implemented. More partnership, less audit.
- Establish a strong line of communication upfront.** Auditing a vendor without proper communication is a good way to start a fight and tee up an adversarial relationship. Make sure to identify key personnel within the organization, such as a technical point of contact that can speak to the control information you need. Maintaining multiple points of contact can keep the process going in the event that your main stakeholder leaves the organization.
- Assign dedicated resources to your program.** Maintaining the above points on prioritization can require a significant amount of time and effort, which are typically not accounted for within third party risk programs. If internal resources cannot be dedicated, leverage an external firm and/or include a tool to speed up the prioritization process.

Now that you understand the core elements of the prioritization process, you are ready to complete a focused assessment for your most important vendors. [NCC Group Third Party Risk Management](#) services help assess the security capabilities of key partners to provide a clear picture of the risks they represent. We invite you to learn more about our services and speak to a security advisor about your risk management needs.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face. To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

www.nccgroup.com