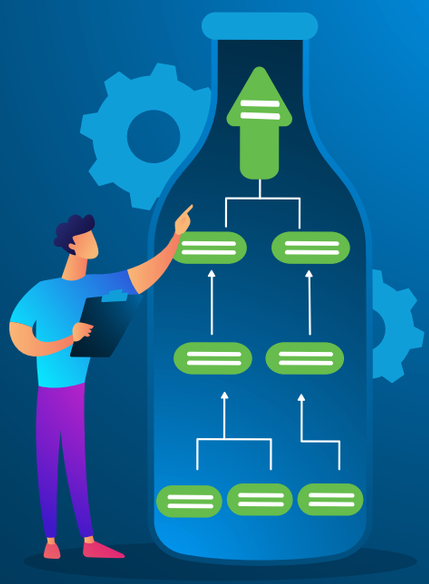
thirdpartytrust

DON'T BE A BOTTLENECK!

A vendor's cheat sheet for responding to security reviews



Are you on the receiving end of vendor risk assessments? Is responding to questionnaires taking too much time, but Sales just keeps pushing? Accelerate your response process and start your customer relationship off on the right foot with these best practices.

✓ DO	× DON'T
Set clear expectations based on specific security standards and frameworks.	Commit to generalities like "reasonable security measures."
Customize your response and be proactive in sharing your latest security documents.	Cast a wide net with generic documentation when a customer asks.
Centralize all of your questionnaires, certifications and attestations, and create a sharing process with clear ownership.	Spread your security documents across repositories and expect different teams to align on a process to share them.

BUILDING A SINGLE, CENTRALIZED SECURITY PROFILE

There's a better way to respond to security reviews than answering one-off spreadsheet questionnaires via email.

Instead of starting from scratch on every assessment, store your security documents in a single, online and centralized repository that you can invite customers to review.

There are tools and solutions available to help you with that!

WHAT DOCUMENTS SHOULD YOU INCLUDE?

- ☑ CIS Controls (Formerly the SANS Top 20 and the CIS Critical Security Controls)
- ☑ Consensus Assessment Initiative Questionnaire (CAIQ)
- ☑ Standardized Information Gathering (SIG)
- ☑ System and Organization Controls (SOC)
- ☑ PCI-DSS
- ☑ Others: Penetration test, cyber insurance, ISO certification, custom FAQs

Let us take your security response process to the next level
thirdpartytrust.com/beacon

3pt Third Party Risk Management Simplified To Scale

sales@thirdpartytrust.com
(872) 256-3192
www.thirdpartytrust.com